Journal of Information Systems and Informatics
Vol. 5, No. 4, December 2023 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v5i4.572 Published By DRPM-UBD

Evaluation the Information Security Management System: A Path Towards ISO 27001 Certification

Jevelin[1], Ahmad Faza[2]

[12]Information System Department, Multimedia Nusantara University, Tangerang, Indonesia
Email: [1]jevelin@student.umn.ac.id, [2]ahmad.faza@umn.ac.id

Abstract

This study addresses the urgent need for robust data security by evaluating the Information Security Management System (ISMS) of a private contractor poised for ISO 27001 certification. It introduces the context of pervasive data breaches that necessitate stringent security measures. Employing a mixed-methods approach, the research method combines the KAMI index for quantitative maturity assessment with qualitative insights from staff interviews and literature reviews. The results reveal the contractor's ISMS maturity at levels I+ to II, indicating a shortfall in meeting the ISO 27001 benchmark. The discussion highlights the efficacy of the PDCA cycle in ISMS implementation, but also underscores the imperative for enhancements to fulfill certification requirements.

Keywords: information security management system, ISO 27001, KAMI index, PDCA method

1. INTRODUCTION

In the realm of information technology, data security has emerged as a paramount concern for companies, particularly with the acceleration of technological advancement [1]. The ubiquity of IT applications necessitates that companies safeguard their data, which supports critical decision-making processes [2]. Yet, companies are confronting a plethora of threats, ranging from data destruction to unauthorized modifications and breaches [4]. The latter, as evidenced by Indonesia's 311 incidents reported by BSSN, poses a severe challenge, especially in sectors like government administration and ICT [5].

Recognizing the importance of data as a corporate asset, a company —a private contractor and developer—is intent on strengthening its defenses against such threats. The path chosen for this fortification is the pursuit of ISO 27001 certification, which requires a preliminary evaluation of the company's Information Security Management System (ISMS). The company opts to utilize

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

the KAMI index as an evaluative tool to gauge its information security maturity in alignment with ISO 27001:2013 standards [5].

This research seeks to fill a notable void in existing literature, which has predominantly centered on the application of the KAMI index and ISO 27001 within various sectors but has seldom drilled down into the niche of private contracting and development [6]-[11]. Unlike prior studies that applied the KAMI index version 4.0, this research advances the methodology by employing version 4.2, reflecting the latest updates and practices [12]. This approach is underpinned by the need to cater to the unique challenges faced by private contractors and developers in securing their information systems. Moreover, the adoption of ISO 27001:2013 as a guiding framework is not arbitrary. This standard is internationally recognized for its comprehensive coverage of principles for maintaining information confidentiality, integrity, and availability, and for offering a systematic approach to managing security risks [13]—imperatives that are especially pressing in the wake of security breaches [14]. By integrating this standard with the updated KAMI index, this study not only explores previously uncharted territory within the contractor and developer sectors but also enriches the discourse on the deployment of advanced tools for ISMS assessment in the contemporary cybersecurity landscape.

2. METHODS

2.1. Research Methods

This study also adopts the PDCA (Plan-Do-Check-Act) method because its processes are valid and effective for implementing ISMS, and it has been a practical approach for many years [15]. The research flow refers to the study conducted by Sundari and Wella in evaluating information security management systems using ISO 27001:2013 and the KAMI (Information Security) index [8]:

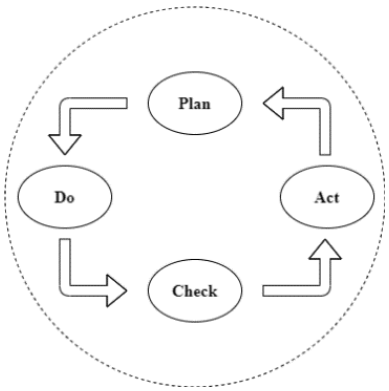

Figure 1 PDCA Method

1. **Cycle: Check**
   In this stage, information about the company's profile, organizational structure, and current information security conditions will be collected through interviews.
2. **Cycle: Act**
   In this stage, the level of information security maturity and compliance with the ISO 27001:2013 standard will be evaluated or measured by completing the KAMI (Information Security) index.
3. **Cycle: Plan**
   After obtaining the evaluation or measurement results, a comparison will be made with the ISO 27001:2013 standard, which will generate recommendations for addressing the deficiencies identified in the company. These recommendations aim to improve the information security management system of the company.
4. **Cycle: Do**
   In this stage, the improvement recommendations will be delivered to the company, serving as a reference for implementing improvements to the company's information security management system.

2.2. The Correlation between ISO 27001 and KAMI Index

BSN (Badan Standardisasi Nasional) has established ISO 27001 as the national standard focusing on information technology, security techniques, and information security management systems. To achieve standardized measurements according to SNI, the National Cyber and Crypto Agency (BSSN) has introduced a tool for evaluating the maturity and compliance of ISO 27001 implementation [7]. This tool is known as the KAMI (Information Security) index. It was initially released in 2009 with version 1.0 and has since been updated and revised to version 4.2. To use the KAMI (Information Security) index, respondents are required to answer provided questions honestly and in line with their company's conditions, ensuring that the KAMI (Information Security) index dashboard displays valid results. The dashboard will display the level of ISO 27001 compliance and the maturity of information security based on the respondents' answers.

Notably, the analysis of KAMI index results reveals a strong correlation with various domains in ISO 27001:2013, encompassing governance, risk management, information security management framework, asset management, and technology and information security. This correlation underscores the index's effectiveness in assessing information security maturity and adherence to ISO 27001:2013 standards. Specific alignments between KAMI (Information Security) 4.2 and Annex A of ISO 27001:2013 further affirm the index's suitability as a tool for measuring ISO compliance and maturity. Figure 2. is a visualization of the correlation between ISO 27001:2013 and the KAMI Index.

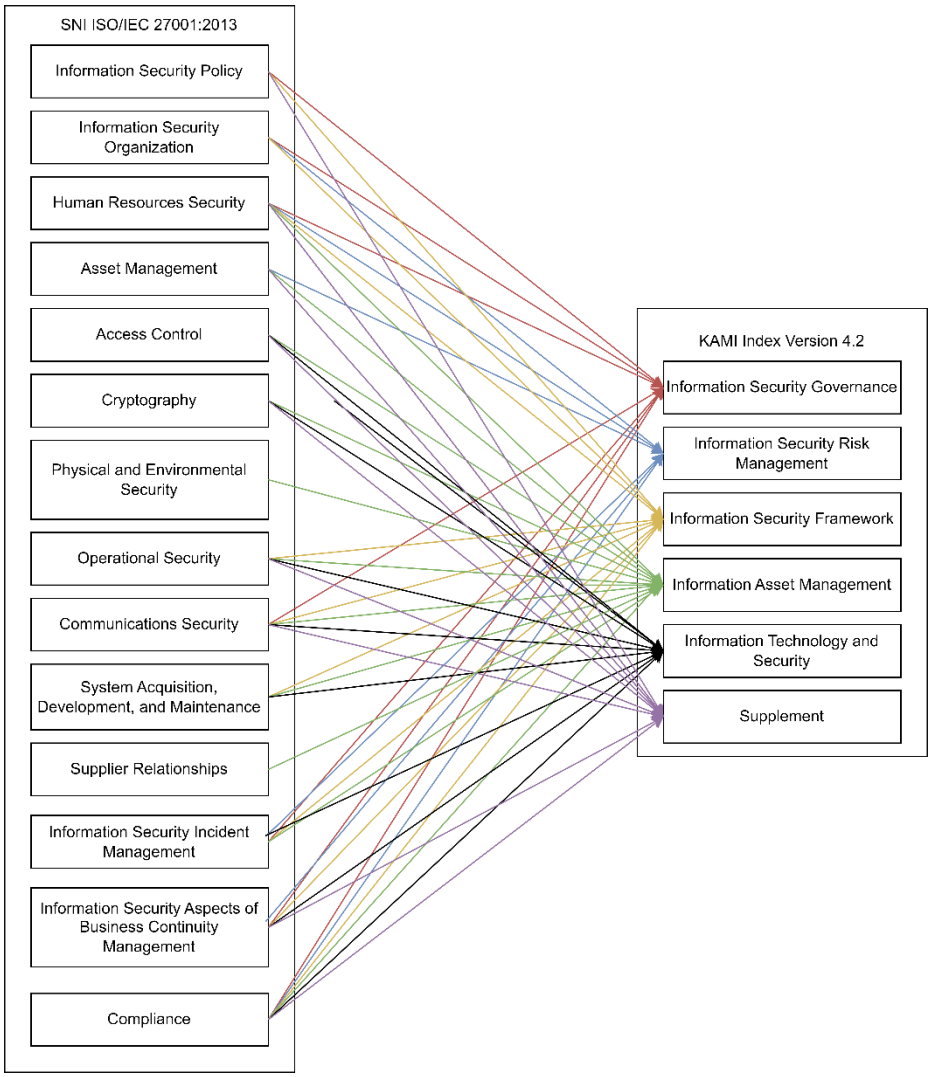

Figure 2. Correlation between KAMI Index 4.2 and ISO 27001:2013

2.3. Data Collection

This research adopts a mixed methods approach, combining quantitative and qualitative data collection and analysis. Quantitative data is obtained through the completion of the KAMI (Information Security) index together with representatives of the comany, while qualitative data is gathered through interviews with one of the staff members, literature review, and recommendations for improvement. Data collection involves online interviews with IT staff members to understand the existing issues and the state of information security

within the company. Additionally, data is collected through a Forum Group Discussion for the completion of the KAMI index, as it measures the maturity level of information security and compliance with ISO 27001:2013. The Forum Group Discussion is conducted online with the head of IT and IT staff members. The data collection period for interviews and the KAMI index questionnaire spans from March 2023 to April 2023.

2.4. Data Analysis Method

This study aims to determine the level of information security maturity and compliance in implementing the ISO 27001:2013 standard. It also seeks to measure the company's dependence on the use of information and communication technology (ICT) and the effectiveness of technology in securing information assets. The calculation of the KAMI (Information Security) index score will be conducted in five areas: information security governance, information security risk management, information security management framework, information asset management, and technology and information security. Additionally, calculations will be performed for the electronic system category and supplements.

3. RESULTS AND DISCUSSION

3.1. Check

Based on direct interviews with one of the IT division staff regarding the current information security condition of the company, it was revealed that the company has not conducted any information security evaluation. However, the company is currently in the preparation phase for ISO 27001 certification to safeguard the company's data and information from security threats such as data breaches.

3.2. Act: Self-Assessment

In this study, a self-assessment will be conducted using the KAMI (Information Security) index tool. The category of electronic systems aims to evaluate the level or category of electronic systems used. The completion of the Electronic Systems Category is based on the current condition of the company. The evaluation results summary of the Electronic Systems Category is presented in Table 1. The summary shows that there are 10 questions, each with 3 answer options. Out of the total of 10 questions, there are 2 questions in category A, resulting in a score of 10 for category A. There are also 6 questions in category B, resulting in a score of 12 for category B. Additionally, there are 2 questions in category C, resulting in a score of 2 for category C. When the scores for categories A, B, and C are added together, the total score for the Electronic Systems Category is 24.

Table 1. Electronic systems category summary

Category	Question	Score
A	2	10
B	6	12
C	2	2
Total	**10**	**24**

The objective of Information Security Governance is to evaluate the readiness of information security governance structure, including the organization/company/function, roles, and responsibilities of information security managers. Table 2. provides a summary of self-assessment for Information Security Governance. Table 3. show that the Company obtained a score of 15 in Stage 1, 28 in Stage 2, and 0 in Stage 3, resulting in a total score of 43 in this area. The maturity level in this area is categorized as I+ because the obtained Level II maturity score has not reached the required score of 36 as defined in the KAMI index. However, the obtained Level II maturity score has met the minimum score requirement of 12. The summary of the obtained evaluation results for the Implementation Status of Information Security Governance is presented in Table 3. Out of a total of 22 answered questions, there are 5 questions categorized as "In Planning," 16 questions categorized as "In Implementation/Partially Implemented," and 1 question categorized as "Fully Implemented.

Table 2. Self-assessment for information security governance

Security Category	Maturity Level				Total Score
	II	III	IV	V	
Stage 1	15	-	-	-	15
Stage 2	18	10	-	-	28
Stage 3	-	-	0	-	0
Total Score	33	10	0	-	43
Maturity Level	I+				

Table 3. Implementation status for information security governance

Implementation Status	Maturity Level				Total
	II	III	IV	V	
Not Performed	0	0	0	0	0
In Planning	3	1	1	0	5
In Implementation / Partially Implemented	9	2	5	0	16
Fully Implemented	1	0	0	0	1
Total	13	3	6	0	22

Information Security Risk Management aims to evaluate the readiness for implementing information security risk management as the basis for implementing information security strategies. Table 4. provides a summary of self-assessment for Information Security Risk Management. Table 4. shows that the score obtained in phase 1 is 19, phase 2 is 12, and phase 3 is 0, resulting in a total score of 31 for the company in this area. The maturity level in this area is categorized as I+ because the obtained maturity level II score has not reached the target score set in the KAMI index, which is 20. However, the obtained maturity level II score has reached the minimum score requirement, which is 14. Table 5. summarizes the results of the evaluation obtained for the implementation status of Information Security Risk Management. Out of a total of 16 questions answered, there are 4 questions categorized as "In Planning," 11 questions categorized as "In Implementation / Partially Implemented," and 1 question categorized as "Fully Implemented".

Table 4. Self-assessment for information security risk management

Security Category	Maturity Level				Total Score
	II	III	IV	V	
Stage 1	19	-	-	-	19
Stage 2	-	8	4	-	12
Stage 3	-	-	-	0	0
Total Score	19	8	4	0	31
Maturity Level	I+				

Table 5. Implementation status for information security risk management

Implementation Status	Maturity Level				Total
	II	III	IV	V	
Not Performed	0	0	0	0	0
In Planning	2	0	2	0	4
In Implementation / Partially Implemented	7	2	0	2	11
Fully Implemented	1	0	0	0	1
Total	10	2	2	2	16

The purpose of the Information Security Management Framework is to evaluate the completeness and readiness of the information security management framework (policies and procedures) and its implementation strategy. Table 6. summarizes the results of the self-assessment of Information Security Management Framework. The score obtained in stage 1 is 18, stage 2 is 28, and stage 3 is 0, resulting in a total score of 46 for the company in this area. The maturity level in this area is I+ because the obtained maturity level II score has not reached the target score set in the KAMI index, which is 24. However, the obtained maturity level II score has reached the minimum score set, which is 15.

Table 7. summarizes the results of the evaluation regarding the implementation status of Information Security Management Framework. Out of a total of 29 questions answered, there are 19 questions categorized as "In Planning" and 10 questions categorized as "In Implementation / Partially Implemented".

Table 6. Self-assessment for information security management framework

Security Category	Maturity Level				Total Score
	II	III	IV	V	
Stage 1	15	3	-	-	18
Stage 2	8	20	-	-	28
Stage 3	-	0	0	0	0
Total Score	23	23	0	0	46
Maturity Level	I+				

Table 7. Implementation status for information security management framework

Implementation Status	Maturity Level				Total
	II	III	IV	V	
Not Performed	0	0	0	0	0
In Planning	3	11	3	2	19
In Implementation / Partially Implemented	8	2	0	0	10
Fully Implemented	0	0	0	0	0
Total	11	13	3	2	29

The objective of Information Asset Management is to assess the adequacy of information asset security, including the entire lifecycle of asset utilization. Table 8. summarizes the results of the evaluation regarding the self-assessment of Information Asset Management. The score obtained in stage 1 is 59, stage 2 is 42, and stage 3 is 12, resulting in a total score of 113 for the company in this area. The maturity level in this area is II because the obtained maturity level II score has reached the target score set in the KAMI index, which is 62. However, this area cannot progress to the next maturity level because the obtained maturity level II score has not reached 80% of the maturity level II threshold, which is 84. Table 8. summarizes the results of the evaluation regarding the implementation status of Information Asset Management. Out of a total of 38 questions answered, there are 4 questions categorized as "Not Implemented," 4 questions categorized as "In Planning," 10 questions categorized as "In Implementation / Partially Implemented," and 20 questions categorized as "Implemented Overall".

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Table 9. Self-assessment for information asset management

Security Category	Maturity Level				Total Score
	II	III	IV	V	
Stage 1	59	-	-	-	59
Stage 2	16	26	-	-	42
Stage 3	-	12	-	-	12
Total Score	75	38	-	-	113
Maturity Level	II				

Table 10. Implementation status for information asset management

Implementation Status	Maturity Level				Total
	II	III	IV	V	
Not Performed	2	2	0	0	4
In Planning	4	0	0	0	4
In Implementation / Partially Implemented	6	4	0	0	10
Fully Implemented	17	3	0	0	20
Total	29	9	0	0	38

The objective of Technology and Information Security is to evaluate the completeness, consistency, and effectiveness of technology utilization in securing information assets. Table 11. presents the scores obtained in stage 1, stage 2, and stage 3, resulting in a total score of 77 for the company in this area. The maturity level achieved in this area is II, as the level II maturity score attained meets the required threshold set in the KAMI index, which is 28. However, this area cannot progress to the next maturity level as the level II score obtained has not reached the 80% threshold of level II maturity, which is 33.6. Table 12. summarizes the evaluation results concerning the implementation status of Technology and Information Security. Out of a total of 26 answered questions, 7 questions are categorized as "In Planning," 10 questions as "In Progress/Partially Implemented," and 9 questions as "Fully Implemented".

Table 11 Self-assessment for supplement

Supplement	Score	Percentage
Third-Party Engagement Security	1.30	43%
Cloud Service Infrastructure Security	0.30	10%
Personal Data Protection	1.69	56%

Table 12 Implementation status for supplement

Implementation Status	Maturity Level			Total
	Third Party	Cloud Service	Personal Data	
Not Performed	0	0	0	0

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Implementation Status	Maturity Level Third Party	Cloud Service	Personal Data	Total
In Planning	3	3	1	7
In Implementation / Partially Implemented	3	7	0	10
Fully Implemented	8	1	0	9
Total	14	11	1	26

3.3. Plan: Comparison of Evaluation Results with ISO 27001:2013

Table 13. shows the percentage achievement scores obtained in the five areas of information security in the KAMI (Information Security) index. The percentage results obtained indicate the extent of achievement in each area. In the table of percentage achievement scores, it is shown that the area with the highest level of achievement is information asset management with a percentage of 67.3%, while the area with the lowest level of achievement is the framework for information security management with a percentage of 28.9%.

Table 13 Percentage of achievement scores

Score	Evaluation	Maximum	Percentage
Information Security Governance	43	126	34.1%
Information Security Risk Management	31	72	43.1%
Information Security Management Framework	46	159	28.9%
Information Asset Management	113	168	67.3%
Technology and Information Security	77	120	64.2%

Figure 3. shows a dashboard and radar chart displaying the evaluation results of the KAMI (Information Security) index at the company. Based on the dashboard and radar chart, the following conclusions can be drawn:

5. The electronic system category at the company obtained a score of 24, indicating a High category, which means that electronic systems are used to support the company's activities.
6. The score obtained for ISO 27001 compliance at the company is 310, falling in the yellow area. Based on this score, the overall evaluation result is Basic Framework Compliance.

7. Among the five areas of information security, the risk management area obtained the lowest score of 31 out of 72, resulting in an achievement level of I+.
8. Among the five areas of information security, the asset management area obtained the highest score of 113 out of 168, resulting in an achievement level of II.
9. In the supplement section, the sub-category with the highest percentage is personal data protection with a percentage of 56%, followed by third-party involvement security with a percentage of 43%. The sub-category with the lowest percentage is cloud service infrastructure security with a percentage of 10%.

Based on the results of the KAMI (Information Security) index, it can be concluded that the level of information security maturity at the company ranges from I+ to II. This indicates that the company is not yet ready for ISO 27001 certification and further improvements are needed to reach the minimum threshold for ISO 27001 certification, which is level III+.

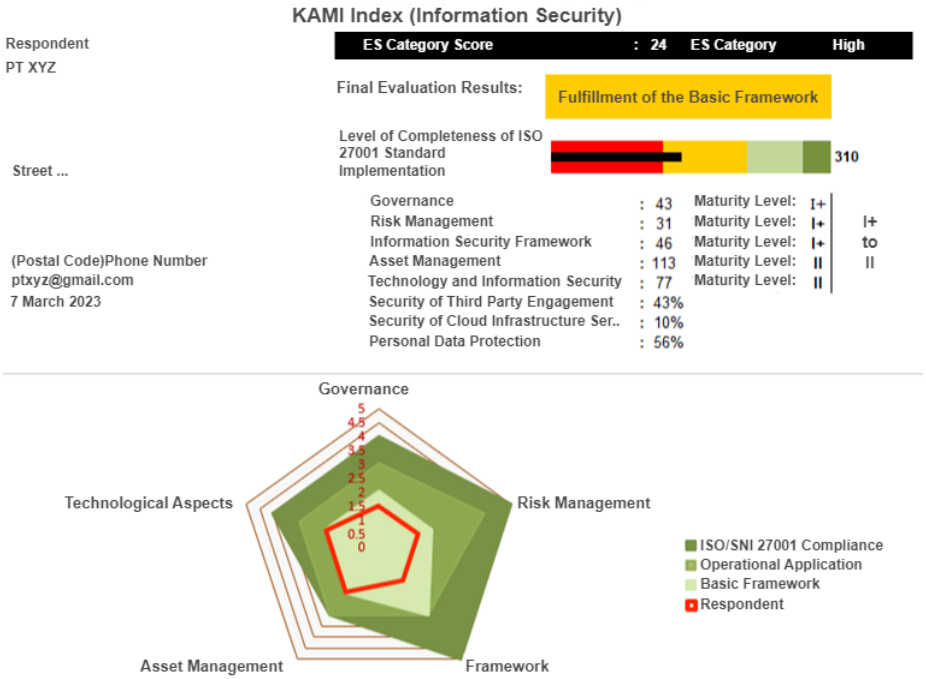

Figure 3 Dashboard and Radar Chart KAMI Index Evaluation Results

Based on the results obtained from the Information Security Index, there are several improvement recommendations to enhance the information security maturity level of the company. Table 14. presents the current condition,

recommendations, and ISO 27001:2013 controls as the basis for formulating the recommendations.

Table 14 Improvement recommendations for areas

Areas	Current Conditions	Recommendations
Information Security Governance	The company does not have a dedicated division or department responsible for managing information security and ensuring compliance.	Establishing a dedicated division responsible for managing information security and ensuring compliance.
	The company has not implemented a socialization program to enhance understanding of information security, including the importance of compliance for all relevant parties.	Implementing a socialization program to enhance understanding of information security, including the importance of compliance for all relevant parties.
	The company has not implemented a program to enhance the capabilities and skills of information security management practitioners.	Implementing a program to enhance the capabilities and skills of information security management practitioners.
Information Security Risk Management	The risk management framework does not include definitions and relationships between the classification level of information assets, threat levels, the likelihood of those threats occurring, and the potential impact or losses that the company may experience.	Develop a risk management framework that includes definitions and relationships between the classification level of information assets, threat levels, the likelihood of those threats occurring, and the potential impact or losses that the company may experience.
	The acceptable threshold for risk levels has not been determined.	Establish the threshold of risk tolerance.
Information Security	Lack of a process to identify information security-threatening situations and	Identifying potential conditions that can threaten information security and

Areas	Current Conditions	Recommendations
Management Framework	categorize them as incidents for further action.	categorizing them as incidents that require follow-up.
	In contracts with third parties, the absence of obligations to report incidents, maintain confidentiality, protect Intellectual Property rights, adhere to usage regulations, and ensure the security of assets and IT services.	Including obligations to report incidents, maintain confidentiality, protect Intellectual Property rights, adhere to usage regulations, and ensure the security of assets and IT services in contracts with third parties.
	Absence of a strategic plan for implementing information security based on risk analysis.	Formulating a strategy for implementing information security based on risk analysis.
Information Asset Management	The document inventory of information assets does not include ownership information.	Include ownership information in the document inventory of information assets.
	There is no document defining the classification of information assets.	Create a document that defines the classification of information assets in compliance with applicable regulations.
	The assessment and categorization process of information assets is not aligned with their importance levels.	Conduct assessment and categorization of information assets based on their importance and security needs.
	There is no definition of access levels and a matrix to record access allocation.	Develop a document that outlines different levels of access for each classification of information assets and a matrix to record access allocation.
	There is no definition of individual responsibilities for information security among all personnel in the company.	Establish a document that defines the individual responsibilities for securing information among all personnel in the company.
	There is no process for investigation and handling	Establish procedures for the investigation process and

Areas	Current Conditions	Recommendations
	of information security incidents.	handling of incidents related to information security.
	There is no process for the relocation of IT assets from their designated positions.	Develop procedures for the process of relocating IT assets.
Technology and Information Security	Implement automatic logging of all changes that occur in the information system.	Create an event log and configure and manage the logging settings.
	Ensure that unauthorized access attempts are automatically recorded in the log.	Create an event log and configure and manage the logging settings to automatically record unauthorized access attempts.
	Perform regular analysis of all logs to identify any security incidents or anomalies.	Establish a regular audit schedule and utilize log analysis tools such as ELK Stack to ensure the accuracy, validity, and completeness of log contents.

3.4. Do: Delivery of Improvement Recommendations

After generating improvement recommendations based on the evaluation results of the Information Security Index (KAMI), the next step is to deliver these recommendations to the company. These improvement recommendations are expected to serve as guidelines for implementing the necessary improvements and strengthening the company's information security management system in preparation for ISO 27001:2013 certification. The final outcome of this stage is the approval sheet for the improvement recommendations, which is signed by the auditor and the auditee.

3.5. Discussion

Based on the evaluation results of the Information Security Index (KAMI), there are several improvement recommendations to enhance the level of information security maturity in the company. Table 15 presents the current condition, recommendations, and ISO 27001:2013 controls as the basis for formulating these recommendations. The self-assessment indicates that the maturity levels in each area have not reached the minimum requirement of Level III+ and the compliance level in implementing ISO 27001:2013 is still in the stage of meeting the basic framework. This suggests that the company is not ready for ISO 27001:2013

certification, necessitating improvement recommendations to enhance the maturity levels in the five areas.

The improvement recommendations for the governance area pertain to roles, responsibilities, and awareness programs aimed at improving understanding, skills, and expertise in information security. For the risk management area, recommendations revolve around the risk management framework and risk tolerance thresholds. In the framework area, recommendations focus on identifying potential threats to information security, contractual obligations with third parties, and the implementation of information security strategies. Regarding information asset management, the improvement recommendations involve documenting asset inventories, defining asset classification, assessing and categorizing information assets based on their importance and security needs, defining access levels and responsibilities, establishing investigation procedures, and implementing asset transfer processes. For the technology and information security area, recommendations relate to log recording and log analysis. Each improvement recommendation has a specific deadline. This allows the company to address the recommendations before the designated deadlines.

This study demonstrates that the Information Security Index (KAMI) can assist companies in measuring their level of information security maturity. This aligns with previous research that utilized the KAMI index to assess information security maturity and completeness in companies [6]–[11]. However, there are differences between this study and previous research, including the research object, the version of the KAMI index, and Annex A. This study focuses on private companies in the contracting and development sector, while previous research examined companies in online shops and distribution sectors. The KAMI index used in this study is version 4.2, while previous research used version 4.0. Another difference lies in Annex A, where this study includes A.5 on information security policies, A.6 on information security organization, A.7 on human resource security, A.8 on asset management, A.9 on access control, A.11 on physical and environmental security, A.12 on operational security, A.14 on system acquisition, development, and maintenance, A.16 on incident management, and A.18 on compliance. In contrast, previous research incorporated A.5 on information security policies, A.6 on information security organization, A.7 on human resource security, A.9 on access control, A.10 on cryptography, A.11 on physical and environmental security, A.12 on operational security, A.13 on communication security, A.14 on system acquisition, development, and maintenance, and A.17 on information security aspects of business continuity management [11].

4. CONCLUSION

This research focuses on evaluating information security management systems using the KAMI (Information Security) index version 4.2. The evaluation results

indicate that the electronic systems category obtained a score of 24, indicating a high level of dependency on information technology (IT) usage in the company's operations. The maturity levels of the five areas in the KAMI index indicate that the company is not ready or suitable for ISO 27001:2013 certification. This is because there are minimum maturity levels that companies need to achieve for ISO 27001:2013 certification. Therefore, recommendations for improvement are necessary for the company to guide the company in enhancing its information security management system. These improvement recommendations are based on the evaluation results using the KAMI index. This research contributes academically by demonstrating the use of the KAMI index to assist organizations in preparing for the implementation of ISO 27001:2013 in the contracting and development industry. From an organizational perspective, this research provides recommendations for ISO 27001:2013 certification readiness in information security systems using the KAMI Index.

REFERENCES

[1] A. P. Idhamani, "Dampak Teknologi Informasi terhadap Minat Baca Siswa," *UNILIB J. Perpust.*, vol. 11, no. 1, pp. 35–41, 2020, doi: 10.20885/unilib.vol11.iss1.art4.

[2] J. Simarmata and others, *Teknologi Informasi dan Sistem Informasi Manajemen*. Yayasan Kita Menulis, 2020.

[3] M. Fianty, A. Angelina, G. Claudia, D. Sertivia, and Jevelin, "Analysis of Factors Affecting Information System Security Behaviour in Employees at IT Company," vol. 13, no. 1, pp. 29–36, 2022, doi: https://doi.org/10.31937/si.v13i1.2660.

[4] I. Y. Sari and others, *Keamanan Data dan Informasi*. Yayasan Kita Menulis, 2020.

[5] "Keamanan siber indonesia 2022." 2022.

[6] A. R. Riswaya, A. Sasongko, and A. Maulana, "Evaluasi Tata Kelola Keamanan Teknologi Informasi Menggunakan Indeks KAMI Untuk Persiapan Standar SNI ISO / IEC 27001 (Studi Kasus : STMIK Mardira Indonesia)," *J. Comput. Bisnis*, vol. 14, no. 1, pp. 10–18, 2020.

[7] P. Sugiarto and Y. Suryanto, "Evaluation of the Readiness Level of Information System Security at the BAKAMLA Using the KAMI Index based on ISO 27001 : 2013," *Int. J. Mech. Eng.*, vol. 7, no. 2, pp. 3607–3614, 2022.

[8] P. Sundari and Wella, "SNI ISO / IEC 27001 dan Indeks KAMI : Manajemen Risiko PUSDATIN (PUPR)," *Ultim. InfoSys J. Ilmu Sist. Inf.*, vol. 12, no. 1, pp. 35–42, 2021.

[9] P. Ferdiansyah, Subektiningsih, and R. Indrayani, "Evaluasi Tingkat Kesiapan Keamanan Informasi pada Lembaga Pendidikan Menggunakan Indeks KAMI 4.0," *J. Mob. Forensics*, vol. 1, no. 2, pp. 53–62, 2019, doi:

https://doi.org/10.12928/mf.v1i2.1001.

[10] I. G. P. K. Juliharta, K. T. Werthi, and N. L. P. N. S. P. Astawa, "Penilaian Keamanan Informasi E-Government Menggunakan Index Keamanan Informasi (KAMI) 4.0," *J. Teknol. Inf. dan Komput.*, vol. 06, no. 02, pp. 238–244, 2020.

[11] A. L. Maryanto, M. N. Al Azam, and A. Nugroho, "Evaluasi Manajemen Keamanan Informasi pada Perusahaan Pemula Berbasis Teknologi Menggunakan Indeks KAMI," *J. SimanteC*, vol. 11, no. 1, pp. 1–12, 2022.

[12] A. Y. Eskaluspita, "ISO 27001 : 2013 for Laboratory Management Information System at School of Applied Science Telkom University," *IOP Conf. Ser. Mater. Sci. Eng.*, pp. 1–6, 2020, doi: 10.1088/1757-899X/879/1/012074.

[13] E. R. Kaburuan and A. Lindawati, "Implementation of Security System on Humanitarian Organization : Case Study of Dompet Dhuafa Foundation," *J. Phys. Conf. Ser.*, 2019, doi: 10.1088/1742-6596/1367/1/012004.

[14] N. V Syreyshchikova, D. Y. Pimenov, T. Mikolajczyk, and L. Moldovan, "Information Safety Process Development According to ISO 27001 for an Industrial Enterprise," *Procedia Manuf.*, vol. 32, pp. 278–285, 2019, doi: 10.1016/j.promfg.2019.02.215.

[15] A. Calder, *ISO27001 / ISO 27002 A Pocket Guide*, Second. IT Governance Publishing, 2013.