Analysis of the Implementation of ISO 27001: 2022 and KAMI Index in Enhancing the Information Security Management System in Consulting Firms

Allisha Apriany*[1], Antoni Wibowo[2]
[1,2]Computer Science Department, Master of Computer Science - Binus Graduate Program, Bina Nusantara University, Jakarta, Indonesia
e-mail: *[1]**allisha.apriany@binus.ac.id**, [2]antoni.wibowo@binus.ac.id

Abstrak

Keamanan Informasi saat ini sudah menjadi hal yang perlu diperhatikan oleh perusahaan agar aset penting perusahaan tetap terjaga dan mendapatkan kepercayaan pelanggan. Dalam operasional sehari-hari, banyak aktivitas dan data pribadi yang dikirimkan ke perusahaan. Akan tetapi, belum banyak perusahaan yang menyadari pentingnya keamanan informasi. Selain itu, hal tersebut dapat menurunkan nilai kompetitif yang tidak mampu melindungi data pribadi pelanggan. Setiap kebocoran data dan pelanggaran keamanan informasi dapat merusak reputasi organisasi. Oleh karena itu, penting untuk memiliki ISMS yang efektif sesuai dengan ISO 27001:2022 yang merupakan standar keamanan informasi internasional yang telah diterapkan pada banyak perusahaan di seluruh dunia. Dalam penelitian ini, penulis akan menilai tingkat kematangan sistem manajemen keamanan informasi berdasarkan ISO 27001:2022 dan Indeks KAMI. Berdasarkan penilaian tersebut, beberapa perbaikan harus dilakukan untuk mencapai tingkat kematangan minimal III+ dari penilaian Indeks KAMI dan berdasarkan ISO/IEC 27001:2022, skor yang diperoleh adalah 39% yang dapat disimpulkan bahwa sebagian besar perusahaan belum menerapkan prosedur apa pun dan beberapa kontrol telah diterapkan. Oleh karena itu, diperlukan rekomendasi perbaikan bagi perusahaan, dimulai dengan penerapan kebijakan dan prosedur terkait manajemen keamanan informasi.

Kata kunci*—ISO27001; Sistem Manajemen Keamanan Informasi; Manajemen Risiko*

Abstract

Electronic Information Security has now become something that needs to be considered by companies so company's important assets are maintained and gain customer's trust. In daily operations, many activities and personal data are sent to the company. However, not many companies are aware of information security. In addition, it can reduce competitive value which unable to protect the personal data of customers. Every data leak and information security breach can damage the reputation of the organization. Therefore, it is important to have an effective ISMS in accordance with the ISO 27001:2022, which is an international information security standard that has been applied to many companies around the world. In this study, the author will assess the maturity level of the information security management system based on ISO 27001:2022 and KAMI Index. Based on this assessment, several improvements must be made to achieve minimum maturity level of III+ from the KAMI Index assessment and based on ISO/IEC 27001:2022, the score obtained was 39% which can be concluded that most companies have not implemented any procedures and some controls have been implemented. Therefore, recommendations for improvement are needed for companies, starting with implementation of policies and procedures related to information security management.

Keywords— *ISO27001; Information Security Management System; Risk Management*

1. INTRODUCTION

The rapid development of the times, especially in the field of technology, creates new challenges for companies to manage information security as best as possible. It is critical to ensure that information security risk management is adequately identified, measured, and monitored. The company tries to avoid gaps that can be penetrated by irresponsible parties. Attempted cyber-attacks continues to occur in company especially malware and SQL injection, which can be detrimental to the company and the company's clients or customers, as well as potentially reducing clients' trust in the company due to the lack of information security implemented by the company. Thus, it is very important to secure information system to ensure the resource or asset [2] of the company are well protected from any kind of threats, such as, worms, hackers, phishers, viruses, and social engineering. ISO 27001 as a reference that provides standard with structurd, cost-effective and systematic way to establish, implement, operate, monitor, review, maintain, and improve information security through the implementation of an Information Security Management System (ISMS). ISO 27001 is a security management system international standard information helps with the information security needs of a government or information agency other needs. It is important to conduct thorough business analyses to support the adoption of ISO/IEC 27001 [3]. ISO 27001 standards and internationally recognized because of its process systematically there are policies, organizational structures and other [4]. In this case, the ISO 27001: 2022 standard is used as a reference for PT XYZ to conduct an assessment of the information security management system. In implementing ICT governance, security factors are a very important aspect to pay attention to to avoid risks [5]. However, ISO 27001 includes information security risk management process which have four stages: Plan, Do, Check, and Act (PDCA) [6]. This stages are defined [7]:

1. Plan - Plan consists of setting goals, vision, and processes to achieve specific results.
2. Do – This stage is for implementing and operating Information Security Management System (ISMS) policies, controls, processes and procedures.
3. Check – this steps is the inspection process where plan and do process monitored and evaluated.
4. Action - In the fourth step, actions are taken to improve results and meet or exceed specifications.

The rapid development of technology presents new challenges for companies to manage information security as effectively as possible. It is crucial to ensure that information security risks are properly identified, measured, and monitored. Companies must work to close any gaps that could be exploited by malicious actors. Cyber-attacks, particularly malware and SQL injections, continue to pose threats to organizations, potentially harming both the company and its clients, and eroding client trust due to inadequate information security measures. Therefore, securing information systems is essential to protect company resources and assets from various threats, including worms, hackers, phishers, viruses, and social engineering attacks. ISO 27001 serves as a standard that provides a structured, cost-effective, and systematic approach to establishing, implementing, operating, monitoring, reviewing, maintaining, and improving information security through the implementation of an Information Security Management System (ISMS). ISO 27001, an internationally recognized information security management system standard, helps address the information security needs of governments, organizations, and other entities. It is essential to conduct thorough business analyses to support the adoption of ISO/IEC 27001 [3]. The ISO 27001 standard is internationally acknowledged for its

systematic approach, incorporating policies, organizational structures, and other elements [4]. In this case, the ISO 27001:2022 standard is used as a reference for PT XYZ to assess its information security management system. In implementing ICT governance, security is a critical factor that must be considered to mitigate risks [5]. The ISO 27001 standard includes a risk management process that follows the Plan, Do, Check, Act (PDCA) cycle [6]. These stages are defined as follows [7]:

1. Plan - Plan consists of setting goals, vision, and processes to achieve specific results.
2. Do – This stage is for implementing and operating Information Security Management System (ISMS) policies, controls, processes and procedures.
3. Check – this steps is the inspection process where plan and do process monitored and evaluated.
4. Action - In the fourth step, actions are taken to improve results and meet or exceed specifications.

This research is to provide an assessment towards the organization's current information security condition, to provide insights and information regarding information security risks, identify the threats and weakness of information security, and give recommendation that can be implemented to enhance the organization's information security management by performing assessment based on ISO 27001:2022 and Indeks KAMI as an tools to assess information security management system in PT XYZ environment. This research was performed by collecting data through direct observations, interviews, and document review to understand the company's information security management system conditions. After that, action needs to be taken to improve information security, starting with developing information security policy and procedure as a basic step to enhance the information security control.

This research aims to assess the organization's current information security status, provide insights into security risks, identify potential threats and vulnerabilities, and offer recommendations to enhance the organization's information security management. The assessment is based on ISO 27001:2022 and Indeks KAMI as tools for evaluating the information security management system in the PT XYZ environment. The research involved data collection through direct observations, interviews, and document reviews to understand the state of the company's information security management system. Following this assessment, actions must be taken to improve information security, beginning with the development of security policies and procedures as foundational steps to strengthen security controls.

2. METHOD

The research will carry out tests on objects according to controls defined. The framework in this research was carried out based on the information security management system standard, namely ISO/IEC 27001: 2022 [8] and Indeks KAMI [9] version 5 that was established by the National Cyber and Crypto Agency (BSSN) has introduced a tool for evaluating the maturity and compliance of ISO 27001 implementation. The assessment of this research performed by collection data or information through direct observation to PT XYZ office, interview with the CEO and staffs that highly engaged with the business-as-usual process and engaged with information security processing. Thr assessment of the ISO 27001: 2022 covering 4 areas of controls domain.

The research conducted tests on subjects based on the controls defined. The framework for this research is based on the ISO/IEC 27001:2022 information security management system standard [8] and Indeks KAMI [9] version 5, introduced by the National Cyber and Crypto Agency (BSSN) as a tool for evaluating the maturity and compliance of ISO 27001 implementation. Data for this research was collected through direct observations at PT XYZ's office and interviews with the CEO and staff members who are closely involved in day-to-day operations and information security processes. The assessment of ISO 27001:2022 covers four areas within the control domains.

Table 1 Domain ISO 27001: 2022

Ref. Annex A	Domain
A.5	**Organizational Control**
A.6	**People Control**
A.7	**Physical Control**
A.8	**Technological Control**

Table 2. shows the assessment conducted in 4 areas of controls. These controls for ISO 27001: 202 are assessed with scoring as below:

Table 2 Assessment Scoring

Maturity Level	Maturity Level	Description	Percentage
0	Non-existant	The company does not aware about the importance or criticality of information technology to be managed well by management	0
1	Initial	The company reactively implements and implements information technology according to existing needs suddenly, without any pre-planning.	20
2	Repetable	The company has a form to repeatedly carried out activities related to the management of information technology governance, but its existence has not been well defined and there are still formal inconsistencies	40
3	Defined	The company has a formal and written standard operating procedure that has been socialized or trained to all levels of management and employees to be adhered to and implemented in daily activities	60
4	Managed	The company has a number of indicators or quantitative measurement that function as targets and performance goals for each application of information technology applications	80
5	Optimized	The company has implemented information technology governance that refers to common best practice	100

However, The assessment of the Indeks KAMI score will be performed in eight areas [10]-[13]:

- Electronic System Category, This section evaluates the level or category of electronic systems used. This electronic system category divided into low, high, and strategic. It represent how high the company to depend on system electronics.

Table 3 System Electronic Category

Low		**Final Score Range**		**Readiness Status**
10	15	0	247	Not feasible
		248	443	Framework Fullfilment
		444	760	Good Enough
		761	916	Good
High		**Final Score Range**		**Readiness Status**
16	34	0	387	Not feasible
		388	646	Framework Fullfilment
		647	828	Good Enough
		829	916	Good
Strategic		**Final Score Range**		**Readiness Status**
35	50	0	472	Not feasible
		473	760	Framework Fullfilment
		761	864	Good Enough
		865	916	Good

- Governance, This section evaluates the readiness of the agency/company's form of information security governance along with the functions, duties and responsibilities of information security managers.
- Risk, This section evaluates the readiness to implement information security risk management as a basis for implementing information security strategies, Framework, This section evaluates the completeness and readiness of the information security management framework (policies and procedures) and its implementation strategy.
- Asset Management, This section evaluates the completeness of the security of information assets, including the entire use cycle of these assets.
- Technology, This section evaluates the completeness, consistency and effectiveness of the use of technology in securing information assets.
- Personal Data Protection, This section evaluates the completeness, consistency and effectiveness of the implementation of security controls related to Personal Data Protection (PDP).
- Supplementary, This section evaluates the completeness, consistency and effectiveness of the implementation of security mechanisms regarding the risk of involvement of external third parties in the agency/company's service delivery operations.

The assessment process is filled in and carried out by providing a list of questions to respondents, then conducting interviews related to information security. Index KAMI v5 assessment or scoring is divided into several categories, which are, “not carried out”, “in planning”, “in implementation/partially implemented”, and “fully implemented” with a score of 0, 1, 2, and 3. Then the total of the number is sum up, and the final results will be obtained for each category. Both assessment tools including ISO 27001: 2022 and Indeks KAMI v5 are used parallelly that are used to assess Information security management system.

3. RESULT AND DISCUSSION

3.1 Result of ISO/IEC 27001: 2022 Assessment

Table 4. shows the percentage of the assessment in the 4 areas. it is shown that the control assessment in Annex 5 scored 38%, control assessment in Annex 6 scored 69% which is highest among other control, control assessment in Annex 7 scored 27% and control assessment in Annex 8 scored 23.5%.

Table 4 shows the percentage of the assessment across the four areas. The control assessment in Annex 5 scored 38%, while the control assessment in Annex 6, the highest among the others, scored 69%. The control assessments in Annex 7 and Annex 8 scored 27% and 23.5%, respectively.

Table 4. ISO/IEC 27001: 2022 Score Result

Annex	Domain	Number of Controls	Assessment Result
A.5	Organizational controls	37	31.8%
A.6	People Controls	8	67.5%
A.7	Physical controls	14	22.9%
A.8	Technological controls	34	18.3%
Average Score			**35.1%**

3.2 Result of Indeks KAMI v5

In the Indeks KAMI version 5 template, there are 8 category of assessment to measure information security controls. First category is related to electronic system category, to assess the level of reliance towards electronic system, with total 10 questions summarize in table 5. The result of the assessment concludes that company have high reliance on system electronics.

In the Indeks KAMI version 5 template, there are eight categories of assessment used to measure information security controls. The first category relates to the electronic system, which assesses the level of reliance on electronic systems. This category includes a total of 10 questions, summarized in Table 5. The results of the assessment conclude that the company has a high reliance on electronic systems.

Table 5 System Electronic Category

Category	Count	Score
A	4	20
B	5	10
C	1	1
Total Score		31
System Electronic Category (Low, High, Strategy)		**High**

Table 6. is the result of assessment related to governance category. Each question is answered with four options, which are “Not Implemented”, “In planning”, “In Implementation/ Partially Implemented” and “Fully Implemented”. Based on the assessment result, there are 8 controls is not implemented, 5 controls in planning, 2 controls in implementation/partially implemented, and 7 controls are fully implemented, with total of 22 controls for governance section resulting score 27. The maturity level in this category result is I+ (Maturity level I+ is defined as “initial condition” for the assessment). To reach maturity level II (Implementation of the Basic Framework), the score of the assessment shall reach minimum 36 as defined in Indeks KAMI v.5.

Table 6 shows the results of the assessment related to the governance category. Each question is answered with one of four options: “Not Implemented,” “In Planning,” “In Implementation/Partially Implemented,” and “Fully Implemented.” Based on the assessment results, 8 controls are not implemented, 5 controls are in planning, 2 controls are in

implementation/partially implemented, and 7 controls are fully implemented, for a total of 22 governance controls, resulting in a score of 27. The maturity level for this category is I+ (defined as "initial condition" in the assessment). To reach maturity level II (Implementation of the Basic Framework), a minimum score of 36 is required, as defined by Indeks KAMI v.5.

Table 6 Result of Assessment Governance Category

Category	Count
Not Implemented	8
In Planning	5
In Implementation/ Partially Implemented	2
Fully Implemented	7
Controls Count	22
Score	27
Maturity Level	I+

The next category is assessment for risk as shown in table 7. Out of 16 controls, there are 6 controls that are not implemented, 3 controls in planning, 6 controls in implementation/ partially implemented, and 1 control that is fully implemented with maturity level as I+.

Table 7 Result of Assessment Risk Category

Category	Count
Not Implemented	6
In Planning	3
In Implementation/ Partially Implemented	6
Fully Implemented	1
Controls Count	16
Score	18
Maturity Level	I+

Table 8. shows the result of assessment for framework category with total 23 controls. Based on the assessment result, there are 9 controls that are not implemented, 12 controls that are in planning, 9 controls in implementation/ partially implemented, and 2 controls that are fully implemented with maturity highest maturity level compared to other category. The maturity level result is II (Implementation of the Basic Framework).

Table 8 Result of Assessment Framework Category

Category	Count
Not Implemented	9
In Planning	12
In Implementation/ Partially Implemented	9
Fully Implemented	2
Controls Count	32
Score	41
Maturity Level	II

Table 9 show the result of assessment for asset management category with total of 53 controls. Based on the assessment result, there are 6 controls that are not implemented, 13 controls that are in planning, 13 controls in implementation/ partially implemented, and 21 controls that are fully implemented with maturity level resulted as I+.

Table 9 Result of Assessment Asset Management Category

Category	Count
Not Implemented	6
In Planning	13
In Implementation/ Partially Implemented	13
Fully Implemented	21
Controls Count	53
Score	131
Maturity Level	I+

Table 10 shows the result of assessment for technology category with total 35 controls. Based on the assessment result, there are 5 controls that are not implemented, 7 controls that are in planning, 15 controls in implementation/ partially implemented, and 8 controls that are fully implemented. The maturity level result is I+.

Table 10 Result of Assessment Technology Category

Category	Count
Not Implemented	5
In Planning	7
s	15
Fully Implemented	8
Controls Count	35
Score	103
Maturity Level	I+

Table 11 shows the result of assessment for framework category with total 49 controls. Based on the assessment result, there are 0 control that are not implemented which represents that company have awareness of privacy data protection, 9 controls that are in planning, 3 controls in implementation/ partially implemented, and 4 controls that are fully implemented with maturity level is I+.

Table 11 Result of Assessment Privacy Data Protection Category

Category	Count
Not Implemented	0
In Planning	9
In Implementation/ Partially Implemented	3
Fully Implemented	4
Controls Count	16
Score	49
Maturity Level	I+

Table 12 shows the result of assessment for supplementary category related to involvement of third parties. this is to evaluate the readiness of Third Party Involvement Security is used according to the existing context or scope. with total of 27 controls. Based on the assessment result, there are 4 controls that are not implemented, 8 controls that are in planning, 10 controls in implementation/ partially implemented, and 5 controls that are fully implemented with maturity level resulted as I+ .

Table 12 Result of Assessment Supplementary Category

Category	Count
Not Implemented	4

In Planning	8
In Implementation/ Partially Implemented	10
Fully Implemented	5
Controls Count	27
Score	53%
Maturity Level	I+

Refer to the results of the information security assessment based on the ISO 27001: 2022 assessment and the Index KAMI v.5. In the ISO 27001: 2022 assessment consisting of 4 Annexes, namely Organizational Control, People Control, Physical Control, and Technological Control, with an average maturity level value of 31. 8%, 67.5%, 22.9%, and 18.3%, respectively. In Organizational control, it shows 31.9% where most of the information security controls for this section is yet to have procedures or policies related to the information security system, or have not been defined, which includes the role and responsibilities of information security, information security management, relationships with stakeholders, threat control, information classification, and so on.

The information security assessment, based on the ISO 27001:2022 framework and the Index KAMI v.5, highlights results across four control areas: Organizational Control, People Control, Physical Control, and Technological Control. The average maturity levels for these controls are 31.8%, 67.5%, 22.9%, and 18.3%, respectively. For Organizational Control, which has a maturity level of 31.9%, most of the information security controls in this area lack formal procedures or policies. This includes aspects such as defining the roles and responsibilities for information security, establishing an information security management system, managing relationships with stakeholders, implementing threat controls, and classifying information.

In the People Control section, the results of the assessment showing 69% which has a high score among all controls. In this case, the company has set policies and procedures for most of the people processes, this shows that the control carried out in the company related to employees in the scope such as screening processes, background checks, training, termination processes, control of confidential data, and others has been carried out, but is not adequate. Next is the physical control process, the assessment results shows 22.8% which represent that the company does not have adequate policies or procedures. In this case, the physical control process needs to regulate policies or procedures to maintain information security in the company, such as controls to maintain access to the data center, safe work areas, equipment management, and others. In the technological control process, the assessment results shows the result as 18.3% where the company needs to establish a policy and procedure related to technology, such as privilege ID control, access to source code, data authentication process, capacity management, protection against viruses, backup data storage process, data loss prevention, and others.

In the People Control section, the assessment results show a maturity level of 69%, the highest among all control areas. This indicates that the company has established policies and procedures for most people-related processes. Controls related to employees, such as screening processes, background checks, training, termination procedures, and the handling of confidential data, have been implemented but are still not fully adequate. Next, the Physical Control section scored 22.8%, indicating a lack of sufficient policies and procedures. The company needs to develop and enforce controls to maintain information security in areas such as data center access, secure workspaces, and equipment management. In the Technological Control section, the assessment results show a maturity level of 18.3%. This underscores the need for the company to establish policies and procedures for managing technology-related controls, such as privileged ID access, source code protection, data authentication, capacity management, antivirus protection, data backup procedures, and data loss prevention, among others.

Other than assessment of ISO 27001:2022, there is also an assessment of the information security based on the Index KAMI which is divided into 8 parts, namely the Electronic System Category, Governance, Risk, Framework, Asset Management, Technology, PDP, and Supplements. From the results of the information security maturity level on the Index KAMI, the figure shows a score of 369 and the final evaluation results are categorized as "not feasible". In the governance and risk management, asset management, technology and information security, personal data protection and third party involvement security sections, the results show a maturity level of I+ which indicates that the level of information security maturity is at "initial status", while for asset management it shows a maturity level, which are categorized as “implementation of the basic framework”. From the assessment results of ISO 27001:2022 and the Index KAMI, both evaluation results show that each assessment tool has the same results, where information security controls using ISO 27001:2022 and the Index KAMI v5 have the same results. In addition, control in the people section in ISO 27001:2022 and control in the information security framework section in the Index KAMI are higher than other control categories. This shows that the information security system is still inadequate to comply with the ISO 27001:2022 standard, so in this case, the company needs to make improvements or improvements in terms of policies and procedures related to information security management, so that with policies and procedures, the company can carry out controls in accordance with those defined in the policies and procedures to enhance its information security management system.

In addition to the ISO 27001:2022 assessment, the company also conducted an information security assessment based on the Index KAMI, which is divided into eight sections: Electronic System Category, Governance, Risk, Framework, Asset Management, Technology, Personal Data Protection (PDP), and Supplements. The Index KAMI assessment resulted in a maturity score of 369, with the final evaluation categorized as "not feasible." In the areas of governance and risk management, asset management, technology and information security, personal data protection, and third-party security, the maturity level was rated as "I+," indicating an "initial status" of maturity. For asset management specifically, the results indicate a maturity level categorized as “basic framework implementation.” Comparing the assessment results of ISO 27001:2022 and Index KAMI, both evaluation tools show consistent findings. Information security controls assessed using ISO 27001:2022 and Index KAMI v5 reflect similar maturity levels. Additionally, the People Control section in ISO 27001:2022 and the Information Security Framework section in Index KAMI scored higher than other control categories. These results indicate that the company’s information security system is still inadequate to meet the ISO 27001:2022 standard. Therefore, the company needs to make significant improvements in its policies and procedures related to information security management. By doing so, the company can ensure that it effectively implements controls as defined in the updated policies and procedures, strengthening its overall information security management system.

4. CONCLUSION

The result of this assessment based on the controls in the ISO 27001: 2022 standard show that in the organizational control domain it is at 31.8%, for the people control domain, it is at 67.5%, for the physical control domain, it is at 22.9%, and finally for the technological control domain, it is at 18.3% with an average overall value of 35.1%. As the result, PT XYZ has mostly not implemented or does not have approved procedures or policies related to information security management, however, there are several controls that have been implemented in the company. The results of the ISMS assessment based on the Index KAMI v.5 which implements information security by fulfilling all security aspects defined by the

ISO/IEC 27001:2022 standard, show that the information security readiness status is still categorized as "not feasible" with a value of 369. Based on the assessment of the Index KAMI v.5, to achieve the readiness status category "Fulfillment of the Basic Framework" with the Electronic System category that has a high level of dependency, it is necessary to achieve a value between 829-916 with a readiness status of "Good". The corrective steps that need to be taken are starting from creating policies and procedures related to the information security management system that cover things that are in the scope of the ISO 27001:2022 standard, namely organizational, people, physical, and technological controls. After the implementation of the policies and procedures was carried out, the researcher tried to re-measure the assessment of the ISO 27001:2022 standard and the Index KAMI. From the assessment results, it shows a fairly significant increase in numbers, where the assessment for control on ISO 27001: 2022 increased from 39% to 92% on average. Meanwhile, the assessment on the WE index increased significantly from the "unworthy" category with a value of 369 to 870 and the information security readiness status increased to "Good" of assessment level based on Index KAMI.

The results of this assessment, based on the controls in the ISO 27001:2022 standard, show that the organizational control domain scored 31.8%, the people control domain scored 67.5%, the physical control domain scored 22.9%, and the technological control domain scored 18.3%, with an overall average of 35.1%. As a result, PT XYZ has largely not implemented or formalized approved procedures or policies related to information security management, though some controls have been applied. The ISMS assessment based on Indeks KAMI v.5, which evaluates information security by aligning with the ISO/IEC 27001:2022 standard, shows that PT XYZ's information security readiness is categorized as "not feasible" with a score of 369. To achieve the readiness status category of "Fulfillment of the Basic Framework" for systems with high dependency, a score between 829 and 916 is required, with a readiness status of "Good." Corrective actions should start with creating policies and procedures related to the information security management system, addressing the areas covered by ISO 27001:2022, namely organizational, people, physical, and technological controls. After implementing these policies and procedures, a reassessment was conducted. The results showed a significant improvement: the ISO 27001:2022 control assessment increased from 39% to an average of 92%, and the Indeks KAMI score rose from 369 ("unworthy") to 870, upgrading the information security readiness status to "Good."

ACKNOWLEDGEMENTS

My sincere gratitude and appreciation to the editorial team, whose careful editing significantly improve the clarity of the study. Also I would like to thank all those who have contributed to the success of this research, I would also like to express my sincere gratitude to my parents, fiancé, and friends, who stood by me, support and encouraged me to work on this study.

REFERENCE

[1] Romanova, A. and Korcek, F. 2023. *The Information Security Management Systems in Business, Journal of Global Information Management*, Vol. 3, 1-29.

[2] Girsang, M., Candiwan., Hendayani, R. Ganesan, Y. 2020. *Can Information Security, Privacy and Satisfaction Influence The E-Commerce Consumer Trust?, International Conference on Information and Communication Technology (ICoICT),* Vol. 8.

[3] Kamil Y., Lund, S., Islam, M. 2023. *Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private*

organizations in Sweden. Information Systems and e-Business Management, Vol. 21, 699-722.

[4] Aurabillah, B., Putri, L., Fadhlilla, N., Wulansari, A. 2024. *Implementasi Framework ISO 27001 Sebagai Proteksi Keamanan Informasi dalam Pemerintahan (Systematic Literature Review), Jurnal Mahasiswa Teknik Informatika*, No. 1, Vol. 8, 454-460.

[5] Riana, E., Sulistyawati, M., Putra, O. 2023. *Analisis Tingkat Kematangan (Maturity Level) Dan PDCA (Plan-DoCheck-Act) Dalam Penerapan Audit Sistem Manajemen Keamanan Informasi Pada PT Indonesia Game Menggunakan Metode ISO 27001:2013, Journal of Information System Research*, No.2, Vol.4, 632-640.

[6] Wibowo, E. and Ramli, K. 2023. *Impact of Implementation of Information Security Risk Management. Indonesia, Journal of Information System*, Vol. 18, 1-17.

[7] Isniah, S., Debora, F., Purba, H. 2020. *Plan do check action (PDCA) method: literature review and research issues, Jurnal Sistem dan Manajemen Industri*, No. 1, Vol. 4, 72-81.

[8] Devi, R., Sensuse, D., Kautsarina, Suryono, R. 2022. *Information Security Risk Assessment (ISRA): A Systematic Literature Review, Journal of Information Systems Engineering and Business Intelligence*, No. 2, Vol. 8, 208-217.

[9] M, Suorsa and P, Helo. 2024. *Information security failures identified and measured – ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis*, *Information Security Journal: A Global Perspective*, No. 3, Vol. 33, 285-306, DOI: 10.1080/19393555.2023.2270984.

[10] ISO/IEC 27002, Information security, cybersecurity and privacy protection, https://www.iso.org/standard/75652.html, access on 15 July 2024.

[11] Božić, V. 2023. *Confidentiality, Integrity and Availibility in hospital*, https://www.researchgate.net/publication/368880457_Confidentiality_Integrity_and_Availibility_in_hospital?enrichId=rgreq-01ddf9f5bb58e9af578623e4e44e2034-XXX&enrichSource=Y292ZXJQYWdlOzM2ODg4MDQ1NztBUzoxMTQzMTI4MTEyMzE1NDE0OEAxNjc3NjU4MzE4NjMz&el=1_x_2&_esc=publicationCoverPdf. Access on 15 July 2024.

[12] Ramadhan, N., Rose, U. 2022. *Adapting ISO/ IEC 27001 Information Security Management Standard to SMEs*, *Information Security*, Luleå University of Technology, Sweden.

[13] Dhahri, S., Sarti, M., Aziz, A. 2017. *Information Security Management System. International Journal of Computer Applications*, No. 7, Vol. 158.

[14] Rosiawan,M. and Trisnawati, J. 2023. *Implementation of Risk Management for Outcome Based Learning, Jurnal Eduscience*, No. 2, Vol. 10, 497-508.

[15] Chandra, N., Ramli, K., Ratna, A., Gunawan, T. 2022. *Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools. Risks*, No. 8, Vol. 10.

[16] Hamdi, Z., et al. 2019. *A Comparative Review of ISMS Implementation Based on ISO 27000 Series in Organizations of Different Business Sectors.* International Conference Computer Science and Engineering, Ser. 1339.

[17] Nurbojatimiko, Susanto, A., Shobariah, E. 2016. *Assessment of ISMS Based On Standard ISO/IEC 27001:2013 at DISKOMINFO Depok City*, *Information System of Science and Technology Faculty, UIN Syarif Hidayatullah,* Jakarta.

[18] ISO/IEC 27001: 2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, https://www.iso.org/standard/27001. Access on 15 July 2024.

[19] Qusef, A., Alkilani, H. (2022). The effect of ISO/IEC 27001 standard over open-source intelligence, PeerJ Comput. Sci., DOI 10.7717/peerj-cs.810.

[20] Roy, P. (2020). A High-Level *Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard*, *Information Management,* University of Washington, Seattle, US.

[21] Alberto, J., Karyati, C. 2023. *Perancangan Sistem Manajemen Keamanan Informasi (SMKI) Berdasarkan ISO 27001: 2022 (Studi Kasus Data Center Dinas Komunikasi dan Informatika Kota Tangerang Selatan)*, *Jurnal Ilmu Komputasi*, No. 4, Vol. 22.

[22] Badan Siber dan Sandi Negara Biro Hukum dan Komunikasi Publik (2023, Aug 2023). *"Konsultasi dan Assessment Indeks KAMI".* https://www.bssn.go.id/indeks-kami/. Access on 17 July 2024.

[23] Juliharta, I., Werthi, K., Astawa, N. 2020, *Penilaian Keamanan Informasi E-Government Menggunakan Indeks Keamanan Informasi (KAMI) 4.0, Jurnal Teknologi Informasi dan Komputer*, No. 2, Vol. 6.

[24] Jevelin, Ahmad, F. (2023), *Evaluation the Information Security Management System: A Path Towards ISO 27001 Certification*, *Journal of Information Systems and Informatics*, No. 4, Vol. 5, 1240-1256.

[25] Sundari, P., Wella. 2021. *SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR). Ultima InfoSys : Jurnal Ilmu Sistem Informasi*, No. 1, Vol. 12, 5-42.