ISSN 2085-4579

Evaluation of Information System Management Security Using Indeks KAMI and Recommendation Based on ISO 27001:2013 at PT XYZ (Travel Agent)

Gavrilla Claudia[1], Wella[2]
[1,2] Program Studi Sistem Informasi, Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara, Tangerang, Indonesia
[1]gavrilla.claudia@student.umn.ac.id
[2] wella@umn.ac.id

Accepted 08 June 2023
Approved 14 July 2023

***Abstract*— PT XYZ is one of the Travel Agent companies in Indonesia that is aware of information security, as shown due to the ISO 27001:2013 certification in 2021. However, there are still areas that must be adjusted to improve the company's Information Security Management System.**

In this study, the CAPD (Check-Act-Plan-Do) technique was used, with the KAMI Index supporting as an information security evaluation tool in compliance with ISO 27001:2013 standards. Check examines the firm's present state, Act evaluates the areas identified in the KAMI Index, Plan analyzes the evaluation outcomes and makes recommendations in accordance with ISO 27001: 2013 and Do offers recommendations to the company.

The results of the evaluation show that PT XYZ received a score of 623 from 645 and the value is in the green area, indicating that it is in the "Good" category. The evaluation findings from PT XYZ's KAMI Index are decent but have not yet achieved the highest rating. To help PT XYZ, maximize the Information Security Management System, its existence is utilized as a finding that is compared to the ISO 27001: 2013 standard and results in recommendations for improvement.

***Index Terms*- KAMI Index, Information Security Management System, ISO 27001:2013.**

I. Introduction

A new period, the technological age, was founded in the 18th century, marking the start of the industrial revolution 4.0, which profoundly impacted human life [1]. The organization utilizes technology in its operations, which has a favourable effect on the business. One of the advantages is the production of information, which can then be transformed into data and used for decision-making to accomplish a company's objectives [2]. However, there are some things that businesses need to be aware of to maintain stability in data production and remain competitive and develop in the technology era. The issue to be aware of is information risk, that threats are something to keep an eye out for because they might prevent decision-making, and information is a vital asset for businesses [3]. Cybersecurity refers to the measures that can be implemented to protect corporate data and assets. Information security is one of the cyber-security methods used to protect firm information [4]. Information security needs to be implemented by a corporation since it is crucial. Three key goals, namely confidentiality, availability, and information integrity, can be achieved in a corporation by applying information security [3].

Evaluation of the Information Security Management System is one of the applications of information security that companies can implement; with companies conducting evaluations, it can be used as a reference for companies in ensuring information security in their companies [5]. A supporting framework or standard is required to guide or point of reference when evaluating an organization's information security management system. ISO 27001 is one model that focuses on Information Security Management Systems.

One of Indonesia's businesses involved in tourism or online travel is PT XYZ, and it is known that the company has obtained ISO 27001: 2013 certification in the area of the Payment Process. During an interview with the company, it was learned that there were still areas of the ISO 27001 certification that needed to be improved. This topic is covered in Annex 6.1.1 of ISO 27001 version 2013, which discusses prospective employees' background checks. With this in mind, PT XYZ is trying to enhance the company's Information Security Management System by carrying out routine evaluations to get certified in the upcoming year.

This research aims to assess the Information Security Management System to evaluate the company's capability and level of maturity related to information security and to offer recommendations for development by ISO 27001:2013 standard. In order to adapt to company conditions, this research was carried out utilizing the CAPD (Check-Act-Plan-Do) technique and the KAMI Index evaluation tool [6].

II. Theoretical Basis

A. Information Security

Information security is the protection of all types of information resources from parties who are not authorized to manage the information, aiming to ensure and guarantee business continuity, lower business risk, and maximise profits or return on investment and business opportunities [7]. According to ISO 27000, three aspects of information security require attention. These aspects are:

1
CONFIDENTIALITY
INFORMATION SECURITY
2
INTEGRITY
3
AVAILABILITY

Figure 1 Information Security Aspect

a. Confidentiality is an aspect that secures the confidentiality of data or information and restricts access to it to those with the necessary authorization.

b. Integrity is an aspect that ensures that data or information cannot be altered without authorization from the relevant authorities.

c. Availability is an aspect that ensures that data or information will always be accessible and may be accessed without any hassle by authorized users whenever and whenever they need it [8].

B. Information Security Management System

Information Security Management System (ISMS) is a management system that implements information security within a business or organization. The Information Security Management System (ISMS) is designed to reduce risk and provide business continuity to lessen security breaches' effects [9].

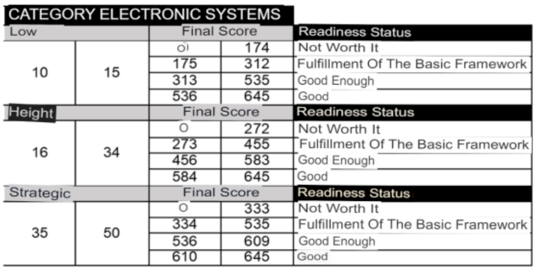
C. ISO 27001

The International Organization for Standardization (ISO) worldwide organizational body created the ISO 27001 standard, which the entire world, including Indonesia, has recognized and adopted [10]. The purpose of ISO 27001 is to guarantee that the chosen security measures can protect information assets from various threats and provide the parties concerned confidence in the degree of security [11]. The ISO 27001 standard itself contains requirements or fundamental prerequisites that must be completed to establish an Information Security Management System (ISMS) within a company. The Plan-Do-Check-Act (PDCA) model, which is utilized as an evaluation method by the Information Security Management System (ISMS), was adopted in the development of ISO 27001 [12].

D. The KAMI Indeks

The KAMI index is a tool to measure both the readiness and maturity of an organization's information security. The KAMI index has been established and adapted to international standards, specifically ISO 27001 version 2013. The KAMI index was also developed so that it may be used by any company or agency, regardless of its size, scope, or level of interest in utilizing ICT to assist in the execution of current business operations. [13].

The KAMI Index questions are divided into two categories of needs. The first is based on the readiness level for implementing safeguards by the completeness of existing controls in ISO 27001:2013 and minimal readiness as a requirement for carrying out ISO 27001:2013 certification. After completing the questions that the company's policies must answer, a score will be calculated to identify the Electronic System's level of readiness, which is further divided into three categories: Low, High, and Strategic [14]. The relationship between readiness status and the type of electronic systems is shown in Figure 2.

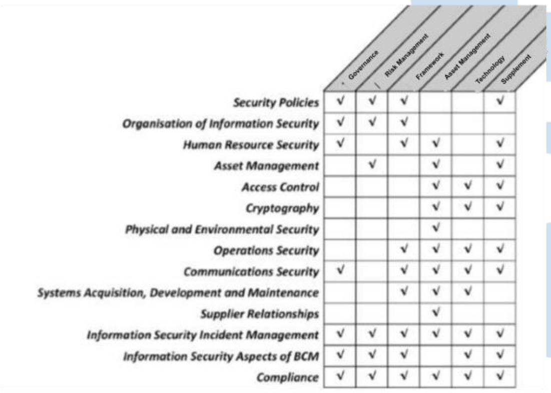


CATEGORY ELECTRONIC SYSTEMS				
Low		Final Score		Readiness Status
10	15	oi	174	Not Worth It
		175	312	Fulfillment Of The Basic Framework
		313	535	Good Enough
		536	645	Good
Height		Final Score		Readiness Status
16	34	O	272	Not Worth It
		273	455	Fulfillment Of The Basic Framework
		456	583	Good Enough
		584	645	Good
Strategic		Final Score		Readiness Status
35	50	O	333	Not Worth It
		334	535	Fulfillment Of The Basic Framework
		536	609	Good Enough
		610	645	Good

Figure 2 Readiness Status Correlation with Electronic System Categories

The second category is based on the maturity level category of security implementation. It includes a category that relates to the level of maturity utilized by the framework or framework that will subsequently be used to characterize the grading of information security readiness inside a firm [13]. To identify the level of maturity in this category, five areas are evaluated by the ISO 27001: 2013 standards for information maturity. The five areas are Information Security Governance, Information Security Risk Management, Information Security Framework, Information Asset Management, and Information Technology and Security.

E. *ISO 27001 relationship with the KAMI Index*



	Governance	Risk Management	Framework	Asset Management	Technology	Supplement
Security Policies	√	√	√			√
Organisation of Information Security	√	√	√			
Human Resource Security	√		√	√		√
Asset Management		√		√		√
Access Control				√	√	√
Cryptography				√	√	√
Physical and Environmental Security				√		
Operations Security			√	√	√	√
Communications Security	√		√	√	√	√
Systems Acquisition, Development and Maintenance			√	√	√	
Supplier Relationships				√		
Information Security Incident Management	√	√	√	√	√	√
Information Security Aspects of BCM	√	√	√		√	√
Compliance	√	√	√	√	√	√

Figure 3 ISO 27001 relationship with the KAMI Index

Figure 3 is a correlation between each area in the KAMI Index based on ISO 27001 version 2013 [15].

III. Method

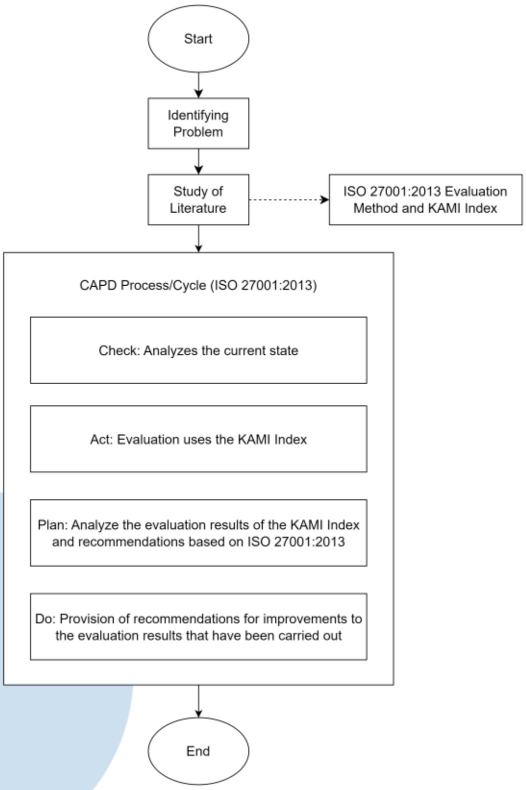

Start
Identifying Problem
Study of Literature
ISO 27001:2013 Evaluation Method and KAMI Index
CAPD Process/Cycle (ISO 27001:2013)
Check: Analyzes the current state
Act: Evaluation uses the KAMI Index
Plan: Analyze the evaluation results of the KAMI Index and recommendations based on ISO 27001:2013
Do: Provision of recommendations for improvements to the evaluation results that have been carried out
End

Figure 4 Research Workflow

The research workflow is depicted in Figure 4. The first stage of this research begins with identifying the problem, followed by a literature review with the related topic of ISO 27001:2013 and the KAMI Index. Additionally, this stage employs the PDCA (Plan-Do-Check-Act) cycle that ISO 27001 adopted. However, this study used a cycle that started with Check-Act-Plan-Do (CAPD), as adopting the CAPD cycle allows it to adapt to business conditions.

The first process, called Check, examines the company's existing state by looking at its structure, profile, and other factors. The second process is the Act, which evaluates an organisation's information security using the KAMI Index. After receiving the evaluation results, the process will proceed to the Plan process, where the evaluation outcomes will be analyzed and compared with the framework reference, namely ISO 27001: 2013. The comparison will result in suggestions for enhancing PT XYZ's information security management system. According to the evaluation that has been done, the final process, Do, is a procedure for making suggestions for improvements to firm information security in line with ISO 27001:2013.

IV. Result and Discussion

The company's electronic systems are evaluated under Category I evaluation, which aims to determine the type or level of the company's employed electronic systems. The KAMI Index is used at PT XYZ to determine the outcomes of the Category I: Electronic Systems evaluation. Whereas the overall score is based on the KAMI Index evaluation for Category I: Electronic Systems, PT XYZ has a score of 41, which is included in the "Strategic" category.

The ISO 27001: 2013 Standard Implementation at PT XYZ scored 623 for completeness based on the KAMI Index evaluation. PT XYZ successfully complies with the completeness requirements for maintaining ISO 27001: 2013 certification, as evidenced by the achievement of this score.

A. *Information Security Governance*

Table 1 Information Security Governance Evaluation

Status	Maturity Level				Total
	II	III	IV	V	
Are not done	-	-	-	-	-
In Planning	-	-	-	-	-
In Application	1	-	-	-	1
Completely Applied	12	3	6	-	21
Total	13	3	6	-	**22**

Table 1 summarizes the conclusions reached during the Category II review. There are 22 questions in Category II, which are broken down into three stages—Stages 1, 2, and 3—and three maturity levels—Stages II, III, and IV. This category has a maximum score of 126.

From a total of 22 questions, at Maturity Level II, there are twelve answers "Completely Applied" and one answer "In Application". At Maturity Level III, there are three "Completely Applied", and at IV Maturity Level, six "Completely Applied" answers.

Based on the evaluation that has been carried out, the company received an evaluation score of 124 which means that the company is at Maturity Level III+ for the Information Security Governance Area. PT XYZ has reached the minimum Maturity Level for Category II: Information Security Governance.

B. *Information Security Risk Management*

Table 2 Information Security Risk Management Evaluation

Status	Maturity Level				Total
	II	III	IV	V	
Are not done	-	-	-	-	-
In Planning	-	-	-	-	-
In Application	4	1	-	-	5
Completely Applied	6	1	2	2	11
Total	10	2	2	2	**16**

Table 2 summaries the findings from the completed Category III evaluation. There are 16 questions that make up Category III, which is broken down into II, III, IV, and V maturity levels as well as stages 1, 2, and 3. The maximum possible score in this category is 72.

From a total of 16 questions, at Maturity Level II, there are four "In Application" and six "Completely Applied" answers. At Maturity Level III, there is one answer, "In Application," and six answers, "Completely Applied"; at Maturity Level IV, there are two answers ", Completely Applied", and at Maturity Level V, there are 2 "Completely Applied" answers.

Based on the evaluation that has been carried out, the company received an evaluation score of 66 which means that PT XYZ is at Maturity Level V for the Information Security Risk Management Area. This was obtained because the company reached Maturity Level IV on the evaluation even though there are still questions that have a score that is not maximal.

C. *Information Security Management Framework*

Table 3 Information Security Management Framework Evaluation

Status	Maturity Level				Total
	II	III	IV	V	
Are not done	-	-	-	-	-
In Planning	-	-	-	-	-
In Application	-	-	-	1	1
Completely Applied	11	13	3	1	28
Total	11	13	3	2	**29**

Table 3 summarizes the findings from the completed Category IV evaluation. There are 29 questions in Category IV, which are broken down into four maturity levels (II, III, IV, and V) and three stages (stages 1, 2, and 3). In this category, the highest possible score is 159.

Of a total of 29 questions, at Maturity Level II, there are 11 answers "Completely Applied". At Maturity Level III, there are 13 answers to "Completely Applied". At Maturity Level IV, there are three answers "Completely Applied", and at Maturity Level IV, there are three answers "Completely Applied", and at Maturity Level IV Maturity V, there is one answer "In Application" and one answer "Completely Applied".

Based on the evaluation that has been carried out, the company received an evaluation score of 156 which means that the company is at Maturity Level IV+ for the Information Security Management Framework Area.

D. *Information Asset Management*

Table 4 Information Asset Management Evaluation

Status	Maturity Level				Total
	II	III	IV	V	
Are not done	-	-	-	-	-
In Planning	-	-	-	-	-
In Application	-	3	-	-	3
Completely Applied	29	6	-	-	35
Total	29	9	-	-	**38**

Table 4 contains a summary of the findings from Table 4 summaries the findings from the completed Category V evaluation. There are 38 questions in Category V, broken down into two maturity levels, II and III, and three stages, namely stages 1, 2, and 3. This category has a maximum score of 168.

Of a total of 38 questions, at Maturity Level II, are twenty-nine answers "Completely Applied". At Maturity Level III, there are three "In Application" and six "Completely Applied" answers.

Based on the evaluation that has been carried out, the company received an evaluation score of 159 which means that the company is at Maturity Level III for the Information Asset Management Area, where Maturity Level III is the maximum maturity level. In addition, the company achieved a minimum score in reaching Maturity Level III in the evaluation even though there were still questions with scores that needed to be more optimal.

E. *Information Technology and Security*

Table 5 Information Technology and Security Evaluation

Status	Maturity Level				Total
	II	III	IV	V	
Are not done	-	-	-	-	-
In Planning	-	-	-	-	-
In Application	-	1	-	-	1
Completely Applied	14	10	1	-	25
Total	14	9	1	-	**26**

Table 5 summarizes the findings from the completed Category VI evaluation. There are 26 questions in Category VI, broken down into 3 phases (phases 1, 2, and 3) and three maturity levels (Stages II, III, and IV). The maximum score for this category is 120.

From a total of 26 questions, at Maturity Level II, there are 14 answers "Completely Applied". At Maturity Level III, there is one answer, "In Application," and six answers, "Completely Applied", and at Maturity Level IV, there is one answer, “Comprehensively Applied".

Based on the evaluation that has been carried out, the company received an evaluation score of 118 which means that the company is at Maturity Level IV for the Information Asset Management Area, where Maturity Level IV is the maximum maturity level. In addition, the company achieved a minimum score in reaching Maturity Level IV in the evaluation even though there were still questions with scores that were not maximized.

F. *Suplemen (Additional Category)*

Table 6 Supplement Category Assessment

Status	Supplement			Total
	Third-Party	Cloud *Service*	Personal Data	
Are not done	-	-	-	-
In Planning	3	1	-	4
In Application	21	4	12	37
Completely Applied	3	5	4	12
Total	27	10	16	**53**

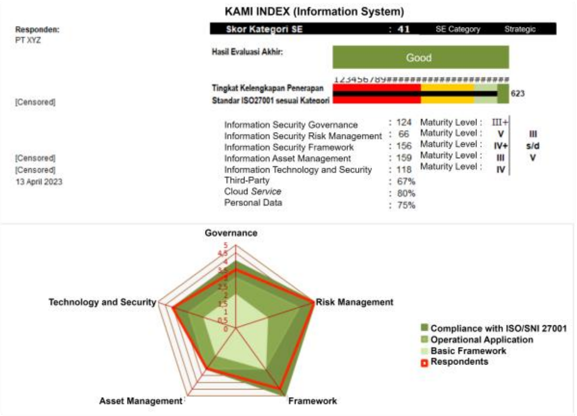
Out of a total of 27 questions in the Securing Involvement of Third-Party Service Provider subcategory, there are three questions with the response "In Planning," 21 questions with the response "In Implementation," and three questions with the response "Completely Implemented" in Table 6. The score that the company received in this subcategory is 2.00. Additionally, of the ten questions in the Cloud Service Security (Cloud Service) subcategory, 1 question has an answer of "In Planning," 4 questions have an answer of "Under Implementation," and five questions have an answer of "Completely Implemented." The score that the company received in this subcategory is 2.40. The Personal Data Protection subcategory has 16 questions, with 12 having "Under Application" and four having "Completely Implemented" as the response. The score that the company received in this subcategory is 2.25.

G. *Achievement Percentage*

Table 7 Percentage of Achievement in 5 Areas

Score	Area I	Area II	Area III	Area IV	Area V
Score	124	66	156	159	118
Max Score	126	72	159	168	120
Percentage	**98,4 %**	**91,7 %**	**98,1 1%**	**94,6%**	**98,4 %**

In the evaluation of the five areas shown in Table 7, it can be seen that PT XYZ's achievement of the maximum achievement score in each area has reached <90%.



KAMI INDEX (Information System)

Responden:
PT XYZ

Skor Kategori SE : 41 SE Category Strategic

Hasil Evaluasi Akhir: Good

Tingkat Kelengkapan Penerapan Standar ISO27001 sesuai Kategori 623

[Censored]

[Censored]
[Censored]
13 April 2023

Information Security Governance	: 124	Maturity Level :	III+
Information Security Risk Management	: 66	Maturity Level :	V
Information Security Framework	: 156	Maturity Level :	IV+
Information Asset Management	: 159	Maturity Level :	III
Information Technology and Security	: 118	Maturity Level :	IV
Third-Party	: 67%		
Cloud *Service*	: 80%		
Personal Data	: 75%		

III s/d V

Figure 5 PT XYZ Dashboard Evaluation

The dashboard shown in Figure 5 indicates that the Electronic System at the company falls under the Strategic category, indicating that Electronic System at the company plays a significant role in assisting the ongoing work process. Additionally, the company earned a 623 overall rating. With this score, the company is now in the positive zone. It is evident from the evaluation's findings that the company complied fully with the completeness requirements for maintaining ISO 27001:2013 certification.

H. *Recommendation*

Recommendations for improvement in maximizing the maturity level of Information Security management at the company in accordance with ISO 27001 version 2013:

Table 8 Recommendations Based on the ISO 27001:2013

No	Current State	Recommendation	ISO 27001:2013 Controls
Information Security Governance			
1.	Not yet defined in detail and complete requirements or security needs and solutions to existing problems.	The company completes documents with requirements or security needs and resolution of problems with responsible parties.	*Clause 5.2 Policy* *Clause 6.1 Actions to address risks and opportunities.* *Clause 7 Support* A.5.1.1 *Policies for information security* A.18.1.1 *Identification of applicable legislation and contractual requirements*
Information Security Risk Management			
1.	Still in the implementation stage to identify threats and weaknesses related to information assets.	The company completes documents that identify threats and weaknesses related to information assets.	*Clause 6.1.2 Information security risk evaluation* A.8.2 *Information classification*
2.	Still in the implementation stage to identify the impact of losses related to the loss or disruption of the main asset function.	The company completes a document that defines the impact of losses related to the loss or disruption of the main asset function.	*Clause 6.1.2 Information security risk evaluation* A.8.1.3 *Acceptable use of assets*
3.	Still in the implementation stage to carry out a structured Information Security risk analysis or study.	Companies are used to implementing structured Information Security risk analysis or studies.	*Clause 6.1.2 Information security risk evaluation* A.18.2.1 *Independent review of information security*
4.	Incomplete documents of risk mitigation and overcoming steps, which are arranged based on priority levels and completion targets and those in charge.	The company completes a document of risk mitigation and overcoming steps, according to priorities, completion targets, and person in charge.	*Clause 6.1.3 Information security risk evaluation* A.6.1.1 *Information security roles and responsibilities* A.8.3 *Media handling* A.16.1 *Management of information security incidents and improvements*
Information Security Framework			
1.	Still in implementation to run a long-term planning program to improve Information Security.	The company sets a schedule and realizes long-term planning to improve Information Security.	*Clause 4.4 Information security management system* *Clause 6.1.2 Information security risk evaluation* *Clause 6.2 Information security objectives and planning to achieve them* *Clause 9.1 Monitoring, measurement, analysis, and evaluation* *Clause 10 Improvement*
Information Asset Management			
1.	Still in the stage of making a list of data or information that needs to be backed up.	The company completes a list of data or information that needs to be backed up.	A.12.3.1 *Information backup*
2.	Still in the stage of making a list of records of Information Security implementation.	The company completes a list of records of Information Security implementation.	*Clause 7.5.3 Control of documented information* A.12.1 *Operational procedures and responsibilities*
3.	Still in the planning stage of making procedures for using information processing devices and securing access to third parties.	The company makes procedures for the use of information processing devices for third parties and ensures access security for third parties.	*Clause 4.3 Understanding the needs and expectations of interested parties.* *Clause 7.3 Awareness* A.9 *Access control*

No	Current State	Recommendation	ISO 27001:2013 Controls
			A.13.2.4 *Confidentiality or nondisclosure agreements*
Information Technology and Security			
1.	Still in implementation to ensure all systems and applications support and implement automatic password changes.	The company ensures that its systems and applications can support the application and change of passwords automatically.	A.9.4.3 *Password management system*

Table 8 recommends improvement for the five KAMI Index components based on the evaluation's findings. The recommendations are made based on ISO 27001 version 2013 standard. Additionally, this recommendation is given to the company with the expectation that the company will implement the recommendation to maximize the Information Security Management System.

V. Conclusion

The following are conclusions from research at PT XYZ that evaluated information security using the KAMI Index:

A. According to Evaluation Category I: Electronic Systems at PT XYZ, the company scored 41, placing it in the Strategic category.

B. The evaluation of PT XYZ's efficiency in the five KAMI Index categories (Governance, Risk Management, Framework, Asset Management, and Technology) reveals that the company has a Good category maturity level, scoring 623 out of 645. According to the results of the evaluation done using the KAMI Index in the area of information security governance, this area receives a maturity level III+, the area of information security risk management, maturity level V, the area of information security management framework, maturity level IV+, the area of information asset management, maturity level III, and the area of technology and information security, maturity level IV.

Results from the previous evaluations led to recommendations for improvement for each KAMI Index aspect. This will enable PT XYZ to implement suggestions to maximize information security at the company.

References

[1] [1] N. J. Harahap, "MAHASISWA DAN REVOLUSI INDUSTRI 4.0," *ECOBISMA (JURNAL EKONOMI, BISNIS DAN MANAJEMEN)*, vol. 6, no. 1, pp. 70–78, Sep. 2019, doi: 10.36987/ecobi.v6i1.38.

[2] M. Andre Alkahfi and Z. M. Nawawi, "Peran Etika Bisnis dalam Perusahaan Bisnis di Era Globalisasi," *ManBiz: Journal of Management and Business*, vol. 1, no. 2, pp. 75–88, Jul. 2022, doi: 10.47467/manbiz.v1i2.1675.

[3] B. Densham, "Three cyber-security strategies to mitigate the impact of a data breach," *Network Security*, vol. 2015, no. 1, pp. 5–8, Jan. 2015, doi: 10.1016/S1353-4858(15)70007-3.

[4] F. A. Anshori and A. R. P. Suprapto, "Perencanaan Keamanan Informasi Berdasarkan Analisis Risiko Teknologi Informasi Menggunakan Metode OCTAVE dan ISO 27001 (Studi Kasus Bidang IT Kepolisian Daerah Banten)," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN*, vol. 2548, p. 964X, 2019.

[5] M. Podrecca, G. Culot, G. Nassimbeni, and M. Sartor, "Information security and value creation: The performance implications of ISO/IEC 27001," Comput Ind, vol. 142, p. 103744, Nov. 2022, doi: 10.1016/j.compind.2022.103744.

[6] P. Sundari and W. Wella, "SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR)," Ultima InfoSys : Jurnal Ilmu Sistem Informasi, pp. 35–42, Jun. 2021, doi: 10.31937/si.v12i1.1701.

[7] P. I. Listyorini and I. Sintya, "SISTEM KEAMANAN SIMRS DI RUMAH SAKIT," in Prosiding Seminar Informasi Kesehatan Nasional, 2021, pp. 234–240.

[8] H. M. J. Saputra, B. S. Sinambela, R. J. Awal, and T. P. Fiqar, "Kebijakan-Kebijakan Iso 17799 Pada Organisasi Sebagai Manajemen Sistem Keamanan Informasi," DoubleClick: Journal of Computer and Information Technology, vol. 3, no. 2, pp. 67–74, 2020.

[9] F. Nasher, "PERANCANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI LAYANAN PENGADAAN BARANG/JASA SECARA ELEKTRONIK (LPSE) DI DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN CIANJUR DENGAN MENGGUNAKAN SNI ISO/IEC 27001:2013," *Media Jurnal Informatika*, vol. 10, no. 1, Jan. 2020, doi: 10.35194/mji.v10i1.465.

[10] N. R. Nia and I. S. Rozas, "STATISTIK PENELITIAN BERBASIS KERANGKA KERJA COBIT, ITIL, DAN ISO 27001 DI INDONESIA," Jurnal Ilmiah Teknologi Informasi dan Robotika, vol. 2, no. 1, pp. 17–23, Jun. 2020, doi: 10.33005/jifti.v2i1.28.

[11] Y. C. Pradipta, Y. Rahardja, and M. N. N. Sitokdana, "Audit Sistem Manajemen Keamanan Informasi Pusat Teknologi Informasi dan Komunikasi Penerbangan Dan Antariksa (PUSTIKPAN) Menggunakan SNI ISO/IEC 27001: 2013," Sebatik, vol. 23, no. 2, pp. 352–358, 2019.

[12] E. W. Yunitasari, "PERBAIKAN SISTEM BELAJAR MAHASISWA PADA MATA KULIAH STATISTIK INDUSTRI DENGAN METODE PLAN DO CHECK ACTION (PDCA)," *IEJST (Industrial Engineering Journal of The University of Sarjanawiyata Tamansiswa)*, vol. 3, no. 2, pp. 64–76, 2019.

[13] H. A. Pratiwi and L. Wulandari, "Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor," Journal of Industrial Engineering & Management Research, vol. 2, no. 5, pp. 146–163, 2021.

[14] BSSN, "Konsultasi dan Assessment Indeks KAMI," Badan Siber dan Sandi Negara. Badan Siber dan Sandi Negara (accessed Mar. 06, 2023).

[15] N. D. Ramadhani, W. H. N. Putra, and A. D. Herlambang, “Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi),” *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN*, vol. 2548, p. 964X, 2020.