Mobile and Forensics
Vol. 6, No. 1, March 2024, pp. 31-38
ISSN: 2714-6685 (online), 2656-6257 (print)
DOI: http://dx.doi.org/10.12928/mf.v1i1.8649

INFORMATION SECURITY READINESS ASSESSMENT AT XYZ AGENCY USING KAMI INDEX 4.2

[1,*]Rigan Rahmadin, [2]Risgi Sri Rahayu, [3]Febrilia Dinda Afriyani
Universitas Amikom Yogyakarta, Indonesia
[1,*]riganrahmadin@students.amikom.ac.id, [2]risgisrirahayu13@students.amikom.ac.id,
[3]dindaafryn5@students.amikom.ac.id
[*]correspondence email

Absract

Dinas Xyz is an agency owned by the government of the Special Region of Yogyakarta (DIY) Province. This agency is responsible for managing activities in a region. This research was conducted to evaluate the level of information security readiness at Dinas Xyz using the KAMI Index 4.2 based on ISO/IEC 27001:2013 criteria. This research involves data collection through interviews and observations, followed by data analysis using the KAMI Index categories. The results showed that Dinas Xyz has a sufficient level of information security readiness, with a score of 285 out of a total of 645. This article provides details of the evaluation results for each category. This research suggests improvements to information security management, especially on cloud storage, to meet the minimum requirements of ISO

Keywords: *KAMI Index 4.2, ISO/IEC 27001:2013, Information Security*

INTRODUCTION

The rapid development of information and communication technology has made vast amounts of information readily accessible. However, this advancement also brings significant risks and potential security gaps. Therefore, it is crucial to prevent data breaches and mitigate risks that could harm institutions or organizations. Information security aims to protect and secure information assets from both internal and external threats, maintaining the confidentiality of personal and corporate data, preventing losses due to security breaches, and safeguarding critical information.

The Information Security Index (KAMI) is a tool used to evaluate the readiness (completeness and maturity) of an organization based on the criteria of SNI ISO/IEC 27001. The KAMI Index, chosen based on the Regulation of the Minister of Communication and Information Technology No. 4 of 2016, provides a flexible framework that necessitates regular evaluation. Evaluation is the process of collecting, analyzing, and assessing data to measure performance, effectiveness, efficiency, or the value of an object. It aims to determine how well an object meets its established goals and offers recommendations for decision-making, improvement, and further development.

Previous research has utilized the KAMI Index to evaluate information security readiness in various organizations. For instance, a study [1] analyzed the East Java Provincial Communication and Information Office, finding maturity levels ranging from I to II and a completeness score of 258. One of the recommendations was related to the information security policy control A.5.1.1. Another study [2] yielded a completeness score of 195, with average maturity levels at I and I+.

This research aims to utilize the improved KAMI Index 4.2 V3 to evaluate the information security readiness of the XYZ Office, a government agency in the Special Region of Yogyakarta

Article History: *Received July 17, 2023; Revised July 27, 2024; Accepted February 30, 2024*

(DIY). The XYZ Office is responsible for managing regional activities, and this study seeks to provide insights into the security and readiness levels of information at this institution.

METHODS

The evaluation of system and information security using the Information Security Index based on ISO/IEC 27001:2013 involves several stages. The research begins with problem identification and a literature review related to system and information security evaluation. This is followed by field studies to collect data through interviews with IT managers at the research site, as well as observation and document review. The reviewed documents are then assessed according to the Information Security Index (KAMI) based on ISO/IEC 27001:2013. The results of this assessment are analyzed to provide recommendations and suggestions for improving information security systems at the XYZ Office according to ISO/IEC 27001 standards.

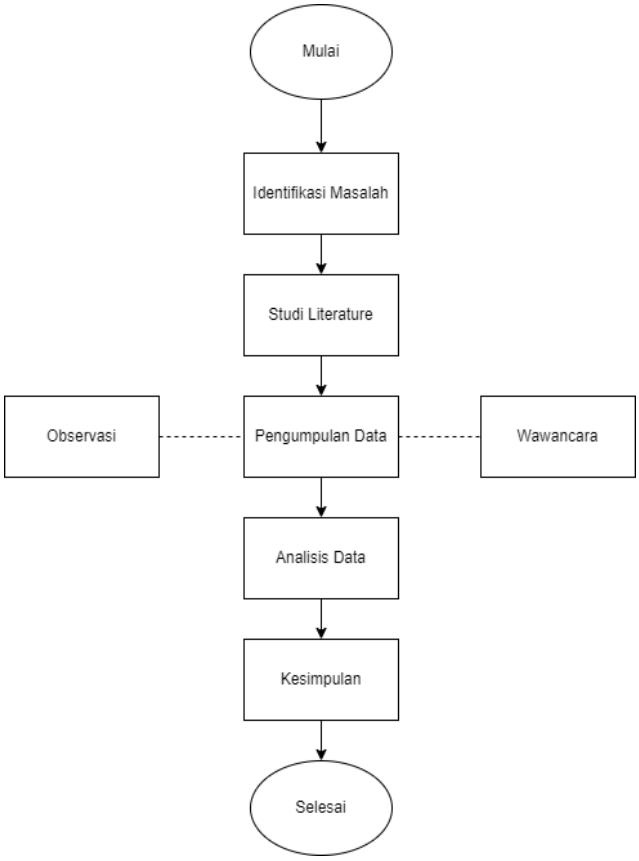

Fig. 1. Research Method Flow

Data Collection

The data collection techniques used in this study follow a quantitative approach, comprising:

1. **Interview Method**: Conduct interviews with those responsible for electronic information services at the XYZ Office, using questions aligned with the Information Security Index.
2. **Observation Method**: Conduct on-site observations at the XYZ Office's secretariat to record and document the existing information technology infrastructure.

Data Analysis

The analysis of the organization's readiness for information security can be performed using computer software or manually. This study involves classifying electronic data to group it into specific categories. The correlation between the categories of the Electronic System and Readiness Status refers to the KAMI Information Security Index, defined in Table 1 [3].

Table 1. Electronic Systems Category

Low		**Final Score**		**Readiness Status**
10	15	0	174	Not Eligible
		175	312	Basic Framework Compliance
		313	535	Good Enough
		536	645	Good
High		**Final Score**		**Readiness Status**
16	34	0	272	Not Eligible
		273	455	Basic Framework Compliance
		456	583	Good Enough
		584	645	Good
Strategic		**Final Score**		**Readiness Status**
35	50	0	333	Not Eligible
		334	535	Basic Framework Compliance
		536	609	Good Enough
		610	645	Good

The classification is further refined based on the maturity level of security implementation, categorized according to the maturity levels used by the COBIT or CMMI frameworks. The KAMI Index defines five maturity levels as follows:

- **Level I -** Initial
- **Level II -** Basic Framework Implementation
- **Level III -** Defined and Consistent
- **Level IV -** Managed and Measured
- **Level V –** Optimal

For a more detailed description, four additional levels are included: I+, II+, III+, and IV+, resulting in a total of nine maturity levels. The minimum threshold for certification readiness according to ISO/IEC 27001:2013 is level III+. The maturity level classification labels are depicted in Figure 1 [3].

Fig. 2. Rentang Tingkat Kematangan

RESULTS AND DISCUSSION

The evaluation of the information security maturity level at XYZ Office, based on seven categories according to the KAMI Information Security Index version 4.0, is presented in Fig. 3. The collected data from each category is summarized in Table 2.

1. Electronic System Category

The Electronic System Category is the first category in the KAMI 4.0 index evaluation document, assessing the level or category of electronic systems used. There are three electronic system categories: low, high, and strategic, with 10 questions in this category. The XYZ Office scored 22, achieving a high category rating. This result indicates that the XYZ Office's electronic system category has a high level of maturity, scoring 22 out of a possible range.

2. Information Security Governance

This category emphasizes the evaluation of the readiness of the information security governance framework, including the roles and responsibilities of information security managers. From the 22 questions posed to respondents, the XYZ Office scored a total of 40, achieving a maturity level of I+. This score is influenced by the minimum threshold score for implementation stages 1 & 2, which is 40, resulting in a score of 0 for implementation stage 3.

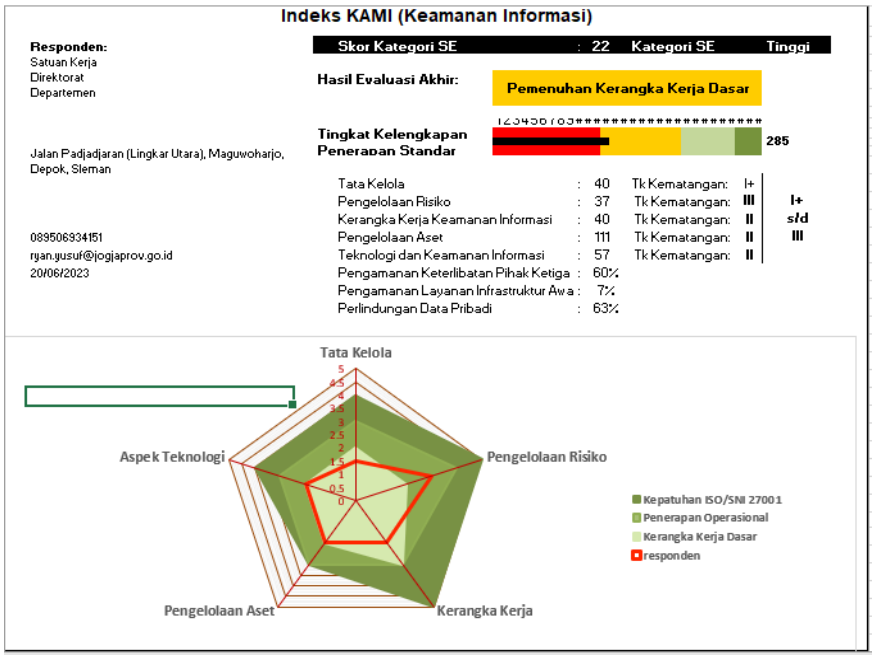

Fig. 3. Dashboard Evaluasi Indeks KAMI 4.2

Table 2. Maturity Level Score

No	Category	Score	Maturity Level
1	Governance	40	I+
2	Risk Management	37	III
3	Information Security Framework	40	II
4	Asset Management	111	II
5	Technology and Information Security	57	II
Score Total		285	Fulfillment of basic framework

Table 3. Information Security Governance Evaluation Results

Development status	Maturity level						
	1	Score	2	Score	3	Score	Total
Not implemented	0	0	0	0	0	0	0
In planning	1	0	2	4	3	0	4
In implementation or partially implemented	2	0	4	12	6	0	12
Completely implemented	3	18	6	6	9	0	24
Total value of information security governance evaluation							40

3. Information Security Risk Management

The evaluation of the information security risk management stage at XYZ Office focuses on assessing the readiness of risk management implementation, which is fundamental to information security strategy implementation. The evaluation resulted in a score of 37, which falls into maturity level III.

Table 4. Information Security Risk Management Evaluation Results

Development status	Maturity level						
	1	Score	2	Score	3	Score	Total
Not implemented	0	0	0	0	0	0	0
In planning	1	1	2	0	3	0	1
In implementation or partially implemented	2	6	4	0	6	0	6
Completely implemented	3	18	6	12	9	0	30

Total value of information security governance evaluation	37

4. Information Security Management Framework

In this stage, the focus is on evaluating the completeness and readiness of the information security management framework (policies and procedures) and their implementation strategy at XYZ Office. This evaluation has two subcategories: the development and management of information security policies and procedures, and the management of information security strategies and programs. The evaluation scored 40, placing it at maturity level II out of 30 questions.

Table 5. Information Security Management Framework Evaluation Results

Development status	Maturity level						
	1	Score	2	Score	3	Score	Total
Not implemented	0	0	0	0	0	0	0
In planning	1	0	2	0	3	0	0
In implementation or partially implemented	2	4	4	0	6	0	4
Completely implemented	3	12	6	24	9	0	36
Total value of information security governance evaluation							40

5. Information Asset Management

This category emphasizes the evaluation of the completeness of information assets, including the entire asset usage lifecycle. The evaluation of this category involves the management of information assets and physical security, with 38 questions posed to respondents. The total evaluation score for asset management is 111, which is classified under maturity level II.

Table 6. Information Asset Management Evaluation Results

Development status	Maturity level						
	1	Score	2	Score	3	Score	Total
Not implemented	0	0	0	0	0	0	0
In planning	1	0	2	0	3	0	0
In implementation or partially implemented	2	6	4	0	6	0	6
Completely implemented	3	45	6	42	9	18	105
Total value of information security governance evaluation							111

6. Information Security and Technology

The evaluation of information security and technology focuses on the completeness, consistency, and effectiveness of technology used in securing information assets at XYZ Office. The evaluation resulted in a score of 57, which falls into maturity level II, indicating a relatively low level of maturity.

Table 7. Information Technology and Security Evaluation Results

Development status	Maturity level						
	1	Score	2	Score	3	Score	Total
Not implemented	0	0	0	0	0	0	0
In planning	1	0	2	0	3	0	0
In implementation or partially implemented	2	4	4	8	6	0	12
Completely implemented	3	24	6	12	9	9	45
Total value of information security governance evaluation							57

7. Supplementary Areas

Pengamanan Keterlibatan Pihak Ketiga : 60%
Pengamanan Layanan Infrastruktur Awan : 7%
Perlindungan Data Pribadi : 63%

Fig. 3. Supplement Evaluation Results

The supplementary areas consist of three parts: third-party involvement security, cloud infrastructure service security, and personal data protection. The evaluation results show that third-party involvement security scored 60%, cloud infrastructure service security scored 7%, and personal data protection scored 63%. The low score of 7% in Cloud Infrastructure Service Security is due to the fact that the systems at XYZ Office are largely centralized at Kominfo, thus XYZ Office only utilizes what is provided. This indicates that while XYZ Office has implemented some aspects of these areas, many aspects of cloud infrastructure service security remain unaddressed.

CONCLUSIONS

The study evaluated the information security readiness of XYZ Office using the Information Security Index (KAMI) based on ISO/IEC 27001:2013 standards. The evaluation encompassed seven categories: Electronic System, Information Security Governance, Risk Management, Information Security Management Framework, Information Asset Management, Technology and Information Security, and Supplementary Areas.

The findings revealed that XYZ Office scored 22 in the Electronic System category, indicating a high maturity level. In the Information Security Governance category, which assesses the governance structure and responsibilities, the office achieved a readiness score of 40, corresponding to a maturity level of I+. For Risk Management, the evaluation resulted in a score of 37, indicating a maturity level of III. In the Information Security Management Framework category, XYZ Office scored 40, with a maturity level of II.

The Information Asset Management category received a score of 111, indicating a maturity level of II. The Technology and Information Security category showed a low maturity level of II, with

a score of 57. The Supplementary Areas evaluation revealed that XYZ Office achieved 60% for third-party involvement security, 7% for cloud infrastructure security, and 63% for personal data protection. The low score in cloud infrastructure security is attributed to the centralized system managed by Kominfo.

Based on the findings, XYZ Office demonstrates strengths in several categories but has significant areas needing improvement, particularly in the governance of information security and cloud storage practices. The final evaluation classifies XYZ Office under the "Basic Framework Fulfillment" category, indicating that it has not yet achieved the minimum threshold required for certification according to ISO/IEC 27001:2013 standards.

REFERENCE

[1] G. Dandy, S. Barani, W. Hayuhardhika, N. Putra, and B. S. Prakoso, "Analisis Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks KAMI (Keamanan Informasi) 4.0 (Studi Kasus : Dinas Komunikasi dan Informatika Provinsi Jawa Timur)," 2020. [Online]. Available: http://j-ptiik.ub.ac.id

[2] N. Diva Ramadhani, W. Hayuhardhika Nugraha Putra, and A. Dwi Herlambang, "Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi)," 2020. [Online]. Available: http://j-ptiik.ub.ac.id

[3] BSSN, "Indeks KAMI," *Badan Siber dan Sandi Negara*, 2021. https://bssn.go.id/indeks-kami/ (accessed Jun. 25, 2023).

[4] F. Kurna, "Evaluasi Adalah: Pengertian, Tujuan, Tahapan, dan Contohnya," *Daily Social*, 2022. https://dailysocial.id/post/evaluasi-adalah (accessed Jun. 25, 2023).

[5] KOMINFO, "Indeks Keamanan Informasi (KAMI)l," *Kominfo*, 2013. https://www.kominfo.go.id/content/detail/3326/indeks-keamanan-informasi-kami/0/kemanan_informasi (accessed Jun. 25, 2023).

[6] S. F. Rahayu *et al.*, "Pengukuran Tingkat Keamanan Informasi Menggunakan Metode Indeks Kami (Studi Kasus: Dinas Komunikasi dan Informatika Kota Pontianak)," 2021.

[7] M. Yunella, A. Dwi Herlambang, W. Hayuhardhika, and N. Putra, "Evaluasi Tata Kelola Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Malang Menggunakan Indeks KAMI," Malang, 2019. [Online]. Available: http://j-ptiik.ub.ac.id

[8] P. Ferdiansyah, S. Subektiningsih, and R. Indrayani, "Evaluasi Tingkat Kesiapan Keamanan Informasi Pada Lembaga Pendidikan Menggunakan Indeks Kami 4.0," *Mobile and Forensics*, vol. 1, no. 2, pp. 53–62, Sep. 2019, doi: 10.12928/mf.v1i2.1001.

[9] 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, doi: 10.7777/jiemar.

[10] W. C. Pamungkas and F. T. Saputra, "Evaluasi Keamanan Informasi Pada SMA N 1 Sentolo Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013," *Jurnal Sistem Komputer dan Informatika (JSON)*, vol. 1, no. 2, p. 101, Jan. 2020, doi: 10.30865/json.v1i2.1924.

[11] A. Kornelia and D. Irawan, "Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1," 2021.