Journal of Information Systems and Informatics
Vol. 5, No. 4, December 2023 e-ISSN: **2656-4882** p-ISSN: **2656-5935**
DOI: 10.51519/journalisi.v5i4.563 Published By DRPM-UBD

Information Security Evaluation Using Case Study Information Security Index on Licensing Portal Applications

Widiastuti Kusumo Wardhani[1], Benfano Soewito[2], Muhammad Zarlis[3]

[1, 2]Computer Science Department-BINUS Graduate Program-Master of Computer Science, Bina Nusantara University, Jakarta, Indonesia 11480
[3]Information System Management Department, BINUS Graduate Program – Master of Information System Management, Bina Nusantara University, Jakarta, Indonesia 11480
e-mail: widiastuti.wardhani@binus.ac.id[1], bsoewito@binus.edu[2], muhammad.zarlis@binus.ac.id[3]

Abstract

The Ministry of Public Works and People's Housing's Licensing Portal application, designed to provide public licensing services, recently faced a significant security breach. The application's webpage was unexpectedly redirected to an online gambling site, which subsequently became the top result in Google searches. This incident not only tarnished the application's reputation but also raised concerns over potential sensitive data theft and disrupted services, causing inconvenience to both the service providers and their customers. In light of these events, and to prevent future occurrences, a comprehensive assessment of the application's security management was conducted using the KAMI Index. This study provided insights into the organization's preparedness for implementing effective information security management. The analysis of these findings led to the development of tailored recommendations for enhancing the application's information security system, aligning with the standards of ISO 27001:2013.

Keywords: Information Security Index, KAMI, Information System Security Assessment, Information System Security, ICT

1. INTRODUCTION

The rapid evolution of communication and information technologies has significantly impacted every aspect of human life [1]. Notably, advancements in computer and Internet technologies have been pivotal in driving the digitalization process, transforming the way we work, communicate, and conduct our daily activities, including online shopping, ticket purchases, ID management, and online licensing [2][3]. The increasing availability of applications on the Internet has led to a surge in their user base [4]. However, this growth has also attracted individuals seeking to exploit application vulnerabilities or user weaknesses for criminal activities [5], underscoring the growing importance of information security in the digital age.

Applications are integral not only to private companies but also to government digital services [6]. Government departments often employ numerous overlapping applications in terms of functionality and data management, complicating security management and increasing vulnerability to threats [7]. This situation is evident in the Ministry of Public Works and People's Housing (PUPR), which has embraced digitalization to streamline work processes, resulting in multiple applications containing sensitive data. Consequently, users of the PUPR's Licensing Portal Application are required to upload sensitive personal data such as NIK, NPWP, phone numbers, photos, certificates, etc. [8], placing a significant responsibility on the Ministry to secure this data.

Notably, the operation of the Licensing Portal application has experienced security breaches, including its redirection to an online gambling site, which gained top ranking in Google searches. These incidents have led to reputational damage, potential data theft from the application servers, and service disruptions, causing inconvenience to both service providers and customers. Pusdatin's IT Security team reports that between July and August 2023, the License Portal application faced 24,967 attacks [9].

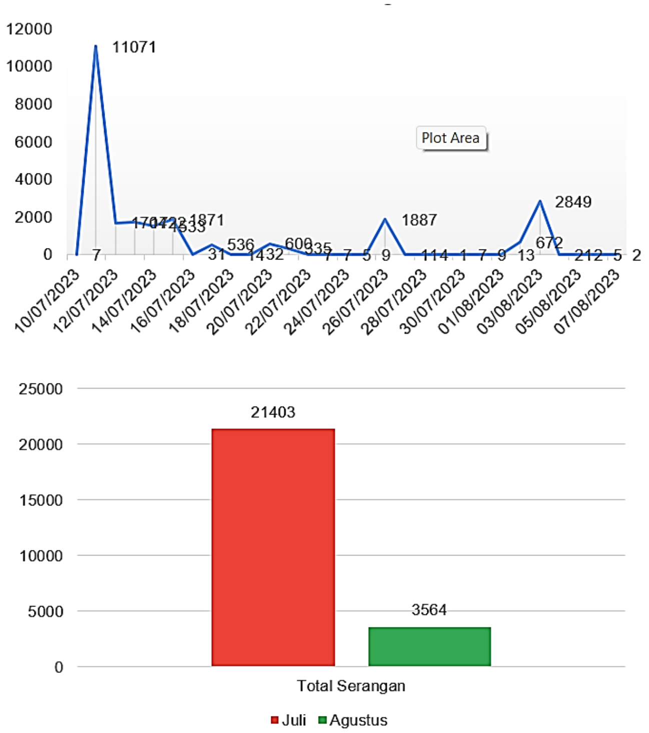


Figure 1. Graphic Of July – August 2023 Attacks on The Licensing Portal Application

To address these challenges, this research aims to evaluate the current state of the application's security management using the KAMI Index. Developed by the Ministry of Communications and Informatics (KOMINFO), the KAMI Index assesses information security maturity in line with the ISO/IEC 27001 standard [10]. This tool evaluates the readiness level, including the maturity and completeness of the information security framework in government agencies. The results of this assessment, indicated by the KAMI Index score, will provide insights into the organization's readiness to implement information security management. These findings will be analyzed to develop recommendations for enhancing the information security system of the PUPR Ministry. The ultimate goal of this research is to assist the Ministry in implementing effective controls and ensuring that its information security management system aligns with international standards for establishing, maintaining, and improving Information Security Management Systems (ISMS) across the organization [6].

2. METHODS

Given the recent unwanted events, there is a potential for similar incidents to recur in the future. Therefore, it is necessary to understand the current state of application management by conducting an assessment. This will involve collecting data through interviews, observations, and document reviews. Information security measures will be evaluated using the KAMI index. Following the evaluation, recommendations will be formulated to enhance the information security system in accordance with ISO 27001 standards.

In this case study, the KAMI index, which adheres to ISO 27001:2013, is employed as a qualitative descriptive method [11]. The KAMI Index serves as a standard evaluation method to assess data security readiness, focusing on ensuring information confidentiality, authenticity, and integrity [12]. Importantly, this evaluation tool is not designed to critique existing security methods, but rather to provide agency leaders with an assessment of the completeness and maturity of their information security framework [13]. The study is divided into several stages, as outlined in the flowchart depicted in Figure 2.

The first phase involves identifying the issues that occurred in the Licensing Portal application. The second stage is a literature review, aiming to gather relevant research and publications to support this study. The third stage is to define the objectives of the research. The outcomes of the evaluation and analysis will be displayed on the KAMI Index dashboard, with recommendations based on these results. The final stage includes drawing conclusions and providing suggestions for the organization and its future research endeavors.

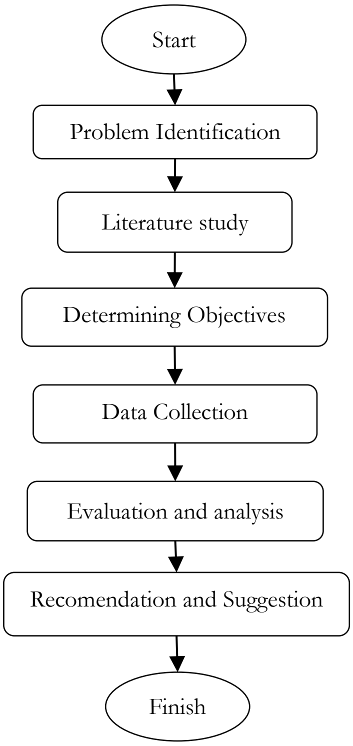


Figure 2. Research Phase Flowchart

For the assessments to be effectively carried out, supporting data are essential. Data collection is conducted through several methods: interviews, observations, and document reviews. Interviews were held at the Data and Information Technology Centre (Pusdatin) with key personnel, including the Head of the Information Technology Management Division, the Sub-Coordinator of Regulation and Licensing, the Sub-Coordinator of Information Security, and the Sub-Coordinator of Infrastructure and Networking. Each of these Sub-Coordinators is responsible for specific duties, and thus, interviews with each were conducted to gather answers relevant to the KAMI index.

Observational data collection involves directly observing the research object. This method aims to identify existing issues and select respondents for the evaluation [14]. Observations will be made within the organizational environment, specifically in areas relevant to the Ministry of PUPR, such as the Central Office's Gate Access, the Pusdatin Building, Working Rooms, Data and Document Storage Areas, On-Premise Data Center (including IT devices inside the data center), IT Storage Room, and utility facilities like the Uninterruptible Power Supply (UPS), Power Generators (Genset), cooling systems, and various cabling and security device installations.

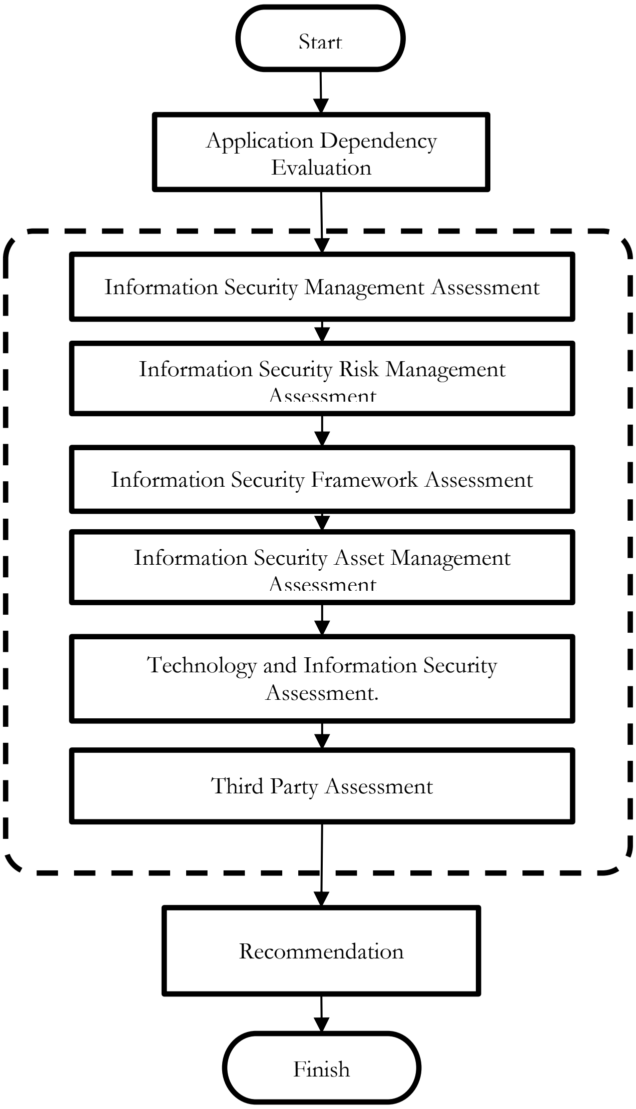

Start
Application Dependency Evaluation
Information Security Management Assessment
Information Security Risk Management Assessment
Information Security Framework Assessment
Information Security Asset Management Assessment
Technology and Information Security Assessment.
Third Party Assessment
Recommendation
Finish

Figure 3. Assessment Steps Flowchart

Document review involves examining internal organizational documents related to the research subject, such as IT Policy, Standard Operational Procedure (SOP) documents, Network Security Log, Application Log, Operating System Security Log, Security Audit Log, Threat Detection Systems Monitoring Log, Access History, Activity History, and System Configuration History. The evaluation process comprises six stages [15]. At this stage, the Licensing Portal Application's information system is measured using the KAMI Index guidelines, issued by the Directorate-General of Informatics Applications and aligning with the SNI

ISO/IEC 27001:2013 Information Security Management System standards (SMKI). This phase is critical as it involves analyzing the data collected and then measuring it using the KAMI Index version 4.2. This measurement is conducted by filling out several evaluation forms as shown in Figure 3.

In this stage, an Assessment of the Application (referred to as Electronic Systems in the KAMI index) is conducted to determine the organization's dependency on the Licensing Portal application. This assessment utilizes a questionnaire completed by respondents, including the Head of Information Technology Management and the Regulatory and License Application Team, as the application's owner and manager. The electronic system category questionnaire comprises 10 questions scored as A = 5, B = 2, C = 1. Based on this scoring, Electronic Systems are categorized into three levels: Low (10 – 15 points), High (16 – 34 points), and Strategic (35 – 50 points). The higher the agency's dependency on the Electronic System, the greater the security level required and to be implemented [8]. The results of this calculation are then used in the KAMI index as outlined in Table 1.

Table 1. Category Of Electronic System Dependencies Score

Category Of Electronic System	
Low	
10	15
High	
16	34
Strategic	
35	50

In the evaluation of five key areas, respondents will be interviewed to complete a survey and provide the necessary supporting evidence. The KAMI index is divided into six sections: Information Security Management, Information Safety Risk Management, Security Frameworks, Information Asset Management, Technology, and Supplement (third party). The questions in the questionnaire are taken directly from the KAMI index.

During the evaluation phase of these five areas, there is a process to validate and analyze the responses and supporting evidence provided by the respondents [10]. The aim is to ensure that the data and evidence are consistent with the actual conditions. To derive the final results, the data will be processed using the pre-defined calculations of the KAMI index. The results of these calculations will be presented in the KAMI index as shown in Table 2.

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

Table 2. Electronic System Connectivity and Information Security Readiness

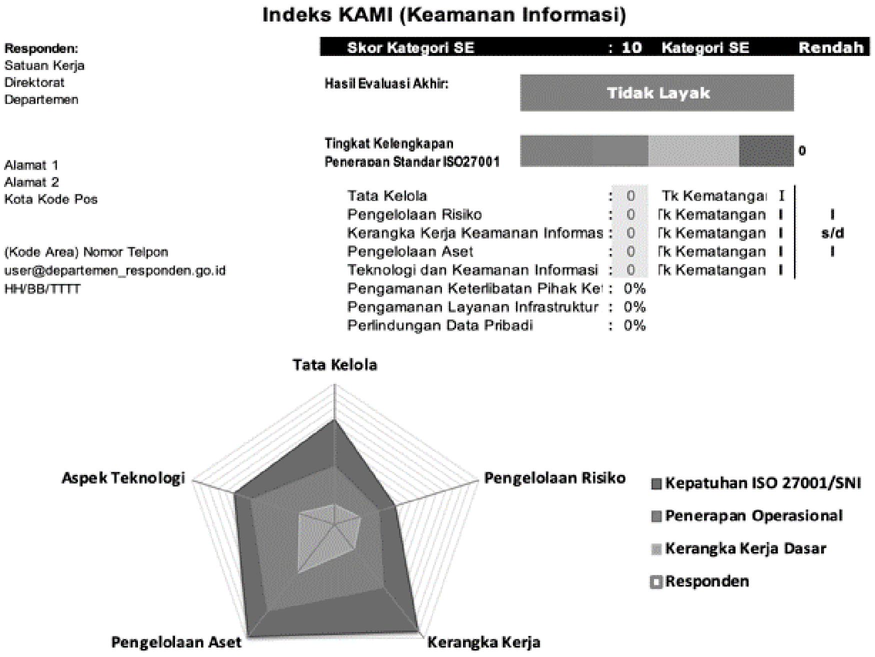
Category of Electronic System				
Low		**Final Score**		**Readiness Status**
10	15	0	174	Ineligible
		175	312	Compliance with the Basic Framework
		313	535	Fair
		536	645	Good
High		**Final Score**		**Readiness Status**
16	34	0	272	Ineligible
		273	455	Compliance with the Basic Framework
		456	583	Fair
		584	645	Good
Strategic		**Final Score**		**Readiness Status**
35	50	0	333	Ineligible
		334	535	Compliance with the Basic Framework
		536	609	Fair
		610	645	Good

After the results are finalized, recommendations will be provided to enhance areas that do not meet the standard. This step is crucial as it identifies specific areas needing improvement and lays out a clear roadmap for achieving compliance with the ISO/IEC 27001 standard. The organization's commitment to implementing these recommendations is expected to significantly elevate its information security practices.

The evaluation framework categorizes the organization's information security readiness based on the maturity level of its security implementation. These levels range from Initial conditions at Level I, where basic security measures are just being established, to Optimal performance at Level V, where security practices are not only implemented but also continually optimized. Each level represents a progressive enhancement in security posture: Basic Framework Implementation at Level II marks the establishment of foundational security controls; Defined and Consistent processes at Level III indicate a systematic approach to security; and Managed and Measured practices at Level IV suggest a mature, monitored, and continuously improving security environment.

The results of the KAMI index evaluation, thoroughly validated and analyzed, will be presented in the form of comprehensive tables and a detailed spider chart, as depicted in Figure 4. These visual representations will provide an at-a-glance understanding of the current security status and areas for improvement.

In the final stage of this case study, the focus shifts to synthesizing the insights gained from the evaluation. Conclusions drawn from the research will highlight key findings, strengths, and vulnerabilities within the organization's information security framework. Based on these insights, strategic recommendations will be formulated, aimed not only at addressing immediate concerns but also at guiding future developments. These recommendations will serve as a blueprint for the organization to enhance its security posture, ensuring that it is well-equipped to handle the evolving challenges in information security and aligns with global best practices.



Indeks KAMI (Keamanan Informasi)

Responden:
Satuan Kerja
Direktorat
Departemen

Alamat 1
Alamat 2
Kota Kode Pos

(Kode Area) Nomor Telpon
user@departemen_responden.go.id
HH/BB/TTTT

Skor Kategori SE : 10 Kategori SE Rendah

Hasil Evaluasi Akhir: Tidak Layak

Tingkat Kelengkapan Penerapan Standar ISO27001 0

Tata Kelola : 0 Tk Kematangai I
Pengelolaan Risiko : 0 Tk Kematangan I
Kerangka Kerja Keamanan Informas : 0 Tk Kematangan I
Pengelolaan Aset : 0 Tk Kematangan I
Teknologi dan Keamanan Informasi : 0 Tk Kematangan I
Pengamanan Keterlibatan Pihak Ke : 0%
Pengamanan Layanan Infrastruktur : 0%
Perlindungan Data Pribadi : 0%

I
s/d
I

Figure 4. Table and Spider Chart KAMI Index
Source: (BSSN, 2021)

3. RESULTS AND DISCUSSION

Based on the calculation of Electronic System Category (SE) values, the PUPR Ministry's Licensing Portal scored 31. The score goes into the High category. The result of the calculation is used with KAMI index as follows on the Table 3.

Table 3. Table of Electronic System Category Value

Category	Amount	Point	Total
Low	1	1	1
High	5	2	10
Strategic	4	5	20
		Total Score	31

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

3.1 Fifth Area of the Information Security Index (KAMI) Assessment

On each rating index there is a number of questions consisting of 3 categories: Category 1 with Not-Executed status scored 0, On Plan status scored 1, Applicable or Partially Implemented Status scored 2, and Comprehensively Executed status scored 3. Category 2 with Not-Executed status scored 0, On Plan status scored 2, Applicable or Partially Implemented Status scored 4, and Comprehensively Executed status scored 6.Category 3 with Not-Executed status scored 0, On Plan status scored 3, Applicable or Partially Implemented Status scored 6, and Comprehensively Executed status scored 9.

In the information security management preparedness section, an assessment of information security functions/ organizations consist of 22 questions was carried out. The result of the calculation is used with KAMI index as follows on the Table 4.

Table 4. Information Security Management Score

Execution Status	Category		
	1	2	3
Not-Executed			
On Plan			1
Applicable or Partially Implemented	7	8	5
Comprehensively Executed	1		
Total Score	82		

The result is 82, obtained from 8 questions in category 1 there are 7 questions answered “Applicable or Partially Implemented”, 1 question answered " Comprehensively Executed". In category 2, out of 8 questions there are 8 questions answered “Applicable or Partially Implemented”. In category 3, out of 6 questions there is 1 question answered "On Plan" and 5 questions replied " Applicable or Partially Implemented". In the Information Security Risk Management section, an assessment is carried out on the Information Safety Risk Study consist of 16 questions. The result of the calculation is used with KAMI index as follows on the Table 5.

Table 5. Risk Management Score

Execution Status	**Category**		
	1	**2**	**3**
Not-Executed			
On Plan			
Applicable or Partially Implemented	10	4	2
Comprehensively Executed			
Total Score	48		

The total value in this section is 48. These values are obtained from 10 questions in category 1, 4 in category 2, and 2 in category 3, with the full answer " Applicable or Partially Implemented ".

In this section, the preparedness of the Information Security Risk Management Framework is assessed in two sections namely the Preparation and Management of Information Security Policies and Procedures consisting of 19 questions, and the Management of Strategy and Information Security Programme comprising of 10 questions. The result of the calculation is used with KAMI index as follows on the Table 6.

Table 6. Risk Management Framework Score

Preparation and Management of Information Security Policies and Procedures			
Execution Status	**Category**		
	1	**2**	**3**
Not-Executed			
On Plan			2
Applicable or Partially Implemented	6	8	2
Comprehensively Executed	1		
II. Information Security Strategy and Program Management			
Execution Status		Category	
	1	2	3
Not-Executed			
On Plan			1
Applicable or Partially Implemented	5	2	2
Comprehensively Executed			
Total Score		98	

The score is 98, obtained of Part I category 1 there are 6 questions answered “Applicable or Partially Implemented”, and 1 question answered "Comprehensively Executed ". In section I of category 2, there are 8 questions answered “Applicable or Partially Implemented”. In section I category 3, there are two questions answered “On Plan” and two questions replied “Applicable or Partially Implemented”. In Part II of Category 1 there are 5 questions answered " Applicable or Partially Implemented". In section II of category 2, there are two questions answered “Applicable or Partially Implemented”. In section II of category 3, there is one question answered “On Plan” and two questions replied “Applicable or Partially Implemented”.

In the preparedness section of Information Asset Management, the assessment is carried out in two parts, namely Information Assets Management, consisting of 27 questions and Physical Security, which consists of 11 questions. The result of the calculation is used with KAMI index as follows on the Table 7.

Table 7. Information Asset Management Score

Asset Management			
Execution Status	**Category**		
	1	**2**	**3**
Not-Executed	2	1	1
On Plan	9	3	1
Applicable or Partially Implemented	6	2	1
Comprehensively Executed	1		
II. Physical security			
Execution Status	Category		
	1	2	3
Not-Executed			
On Plan	2	2	
Applicable or Partially Implemented	3	2	1
Comprehensively Executed	1		
Total Score	61		

The value obtained is 61, because in Part I of Category 1 there are 2 questions answered “Not-Executed”, 9 questions replied “On Plan”, 6 questions replies “Applicable or Partially Implemented”, and 1 question replied "Comprehensively Executed ". In section I of category 2, there is one question answered “Not-Executed”, three questions answered "On Plan”, two questions replied “Applicable or Partially Implemented”. In section I of category 3, there is one question answered "Not done", one question replied "On Plan", and one question responded "Applicable or Partially Implemented ". In section II of category 1, there are 2 questions answered “On Plan”, 3 questions replied “Applicable or Partially Implemented”, and 1 question replied " Comprehensively Executed". In section II of category 2, there are two questions answered “On Plan”, and two questions replied “Applicable or Partially Implemented”. In section II of category 3 there is one question answered “Applicable or Partially Implemented”.

In the Technology and Information Security section, an assessment of Technology Security consist of 26 questions was conducted. The result of the calculation is used with KAMI index as follows on the table 8.

Table 8. Technology Score

Execution Status	**Category**		
	1	**2**	**3**
Not-Executed			
On Plan	3	3	1

Execution Status	Category		
	1	2	3
Applicable or Partially Implemented	11	7	
Comprehensively Executed			1
Total Score		62	

The value obtained is 62, obtained from 14 questions in category 1 there are 3 questions answered “On Plan” and 11 questions replied “Applicable or Partially Implemented”. In category 2, out of 10 questions there are 3 questions answered “On Plan” and 7 questions replied “Applicable or Partially Implemented”. In category 3, out of 2 questions there is 1 question answered "On Plan" and 1 question replied " Comprehensively Executed ".

3.2 Supplement Assessment

In the Supplement section, the assessment was carried out in three sections: Third-Party Service Provider Engagement Security consisting of 27 questions, Cloud Infrastructure Service Security comprising of 10 questions. Personal Data Protection consists of 16 questions.

The results of the calculation in this section of the Supplement are only a percentage of the performance, not resulting in a score to be counted into the evaluation results. The result of the calculation is used with KAMI index as follows on the Table 9.

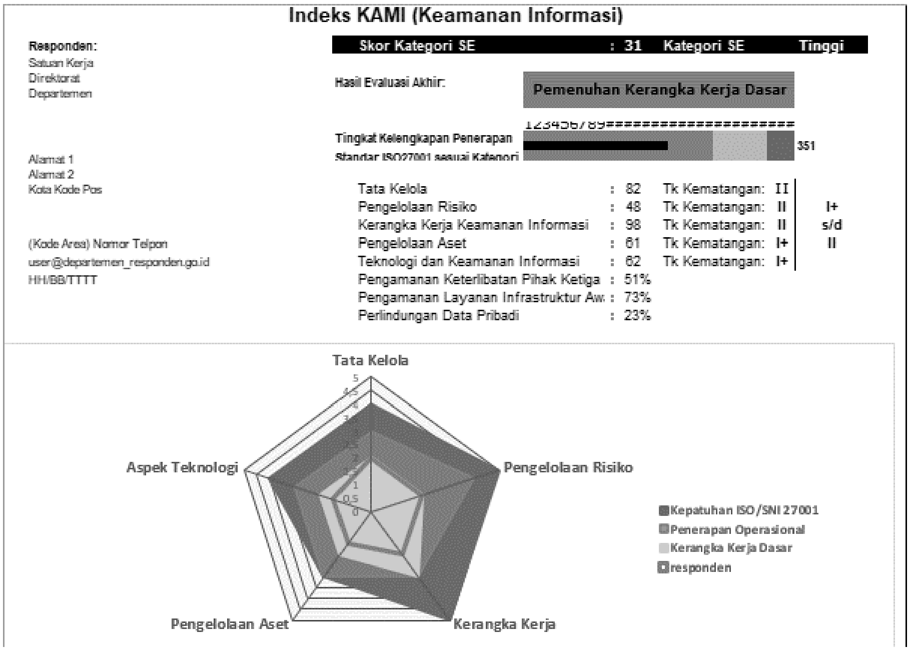
Table 9. Supplement Index

Execution Status	Supplement Ares		
	I	II	III
Not-Executed	6		7
On Plan	6	3	7
Applicable or Partially Implemented	10	2	2
Comprehensively Executed	5	5	
Total Percentage	51%	73%	23%

The percentage of third-party service provider engagement security implementation evaluation results is 51%, the percentages of cloud infrastructure security services implementation assessment results are 73%, and the evaluation of personal data protection implementation is 23%.

3.3 Assessment Results

The final evaluation results using KAMI Index version 4.2 are displayed on the values dashboard and the Radar Chart contains the evaluation values of each section and the readiness status as shown in Figure 5.



Indeks KAMI (Keamanan Informasi)

Responden:
Satuan Kerja
Direktorat
Departemen

Alamat 1
Alamat 2
Kota Kode Pos

(Kode Area) Nomor Telpon
user@departemen_responden.go.id
HH/BB/TTTT

Skor Kategori SE : 31 Kategori SE Tinggi

Hasil Evaluasi Akhir: Pemenuhan Kerangka Kerja Dasar

Tingkat Kelengkapan Penerapan Standar ISO27001 sesuai Kategori 123456789##################### 351

Tata Kelola	:	82	Tk Kematangan:	II	
Pengelolaan Risiko	:	48	Tk Kematangan:	II	I+
Kerangka Kerja Keamanan Informasi	:	98	Tk Kematangan:	II	s/d
Pengelolaan Aset	:	61	Tk Kematangan:	I+	II
Teknologi dan Keamanan Informasi	:	62	Tk Kematangan:	I+	
Pengamanan Keterlibatan Pihak Ketiga	:	51%			
Pengamanan Layanan Infrastruktur Aw.	:	73%			
Perlindungan Data Pribadi	:	23%			

Figure 5. Evaluation results on KAMI index dashboard version 4.2

From Figure 5 the Electronic System category gets a score of 31 which means entering the High category. In the Information Security Management Division, the score is 82, at maturity level II. In the Information Security Risk Management Division, the score is 48, at maturity level II. The Information Security Risk Management Framework the score is 98, at maturity level II. The Information Asset Management Division scored 61, at maturity level I+. The Division of Technology and Information Security scored 62, at maturity level I+. In the Supplement Section, the implementation of the Third-Party Service Provider Engagement Security is 51%, the cloud Infrastructure Service Security implementation is 73%, and the application of the Personal Data Protection is 23%. From the evaluation using the KAMI index version 4.2, the total score is 351 with the predicate of Basic Framework Completion and is at the Level of Compliance I+ to II.

3.4 Discussion

KAMI index assessment reveals critical insights into its information security state. A particularly striking finding is the Ministry's heavy reliance on the Portal License application for its daily operations, as indicated by a usage level of 31 out of a possible 50. This high dependency underscores the application's integral role within the Ministry's workflow and highlights the necessity of a robust and secure IT infrastructure. Ensuring uninterrupted service delivery and safeguarding sensitive data must be top priorities, given the application's central role in the Ministry's functions.

The overall evaluation score of 351 points to significant areas needing improvement in the Ministry's information security practices. This score reflects a basic level of security infrastructure, raising concerns about the Ministry's readiness to handle sophisticated cyber threats. The need for immediate testing and review of the Disaster Recovery Plan (DRP) is particularly alarming, as it suggests potential vulnerabilities in the Ministry's ability to respond effectively to crisis scenarios. Additionally, conducting thorough financial and infrastructure analyses is crucial to support and facilitate the implementation of the recommended security measures.

In the realm of asset management, the Ministry faces several challenges that require comprehensive improvements. These include the implementation of system and process change management, enhanced security controls for computing devices, and stringent guidelines for software installation, data usage, and electronic identity management. Additionally, the establishment of detailed record-keeping practices, along with guidelines for third-party device processing and remote working, is necessary. Developing specific protocols for securing critical areas, such as server and archive rooms, is also essential to protect sensitive information from unauthorized access and potential breaches.

The technology domain presents another set of challenges for the Ministry. Recommendations in this area emphasize the need for standard system security configurations and regular compliance analyses. Implementing automated logging of system changes and effective password management strategies will bolster the Ministry's defenses against cyber threats. Moreover, introducing time-limited access to systems and applications, complemented by robust audit trails for antivirus updates and incident responses, will enhance overall security. The implementation of precise time synchronization mechanisms and secure development environments for application testing are also crucial steps towards achieving a higher standard of information security.

Finally, the current overall security level of the Ministry, at Level I+ to II, indicates only a basic fulfillment of the framework and a significant gap from the ideal Level III+ (Defined and Consistent) as per ISO 27001:2013 standards. This gap underscores the Ministry's urgent need to elevate its information security practices to meet international standards. The assessment of five areas, resulting in a score of 351 and an electronic system usage rate of 31, clearly indicates that the Ministry has yet to comply with the required information security standards set by ISO 27001:2013. Therefore, the Ministry must prioritize enhancing its information security management to protect its assets optimally and ensure the continuity and reliability of its services.

4. CONCLUSION

The detailed analysis conducted in this study reveals that the Ministry of Public Works and People's Housing (PUPR) currently operates at a Basic Framework level in terms of information security. This positioning places the Ministry at a heightened risk of cybercrimes and potential disruptions to its information system services. The high dependency on the Portal License application, as evidenced by a usage level of 31 out of 50, further amplifies these risks, making the need for robust security measures even more critical.

The Ministry's overall evaluation score of 351 in the KAMI index assessment underscores the urgent need for comprehensive improvements across various areas of information security. Key areas requiring immediate attention include the Information Security Framework, Asset Management, and Technology. The necessity for testing and reviewing the Disaster Recovery Plan (DRP), coupled with the implementation of enhanced security controls and guidelines, highlights the existing gaps in the Ministry's preparedness for handling security threats and emergencies.

Moreover, the current security level of the Ministry, which hovers between Level I+ and II, indicates a basic implementation of security frameworks, significantly lagging behind the ideal Level III+ (Defined and Consistent) as per the ISO 27001:2013 standards. This gap signifies a critical need for the Ministry to advance its information security practices. Enhancing these practices is not only about meeting international standards but also about ensuring the safety and confidentiality of sensitive data, maintaining uninterrupted service delivery, and safeguarding the integrity of the Ministry's operations.

Therefore, the Ministry is compelled to undertake a strategic overhaul of its information security management systems. This overhaul should aim to align with the ISO 27001:2013 standards, thereby establishing a more resilient, secure, and trustworthy digital environment. Implementing these changes will require a concerted effort across all levels of the Ministry, involving stringent policy enforcement, regular security audits, and continuous staff training in cybersecurity best practices.

REFERENCES

[1] S. F. Rahayu *et al.*, "Pengukuran Tingkat Keamanan Informasi Menggunakan Metode Indeks KAMI (Studi Kasus: Dinas Komunikasi Dan Informatika Kota Pontianak)," *Coding J. Komput. dan Apl.*, vol. 09, no. 03, pp. 468–477, 2021.

[2] M. Lenawati, W. W. Winarno, and A. Amborowati, "Tata Kelola Keamanan Informasi pada PDAM Menggunakan ISO/IEC 27001:2013 dan COBIT

5," *Sentra Penelit. Eng. dan Edukasi*, vol. 9, no. 1, pp. 44–49, 2017.

[3] P. Februari and F. Fitria, "Audit Sistem Keamanan Informasi Menggunakan ISO 27001 pada SMKN 1 Pugung, Lampung," *POSITIF J. Sist. dan Teknol. Inf.*, vol. 5, no. 2, p. 97, 2019, doi: 10.31961/positif.v5i2.833.

[4] A. P. Putra and B. Soewito, "Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 4, pp. 625–633, 2023, doi: 10.14569/IJACSA.2023.0140468.

[5] M. Nawir, I. AP, and F. Wajidi, "Integration Of Framework Iso 27001 And Cobit 2019 In Smart Tourism Information Security PT. YoY International Management," *J. Komput. dan Inform.*, vol. 10, no. 2, pp. 122–128, 2022, doi: 10.35508/jicon.v10i2.7985.

[6] T. S. Putri, N. Mutiah, and D. Prawira, "Analisis Manajemen Risiko Keamanan Informasi Menggunakan Nist Cybersecurity Framework dan ISO/IEC 27001:2013 (Studi Kasus: Badan Pusat Statistik Kalimantan Barat)," *Coding J. Komput. dan Apl.*, vol. 10, no. 2, pp. 237–248, 2022.

[7] S. Nurul, S. Anggrainy, and S. Aprelyani, "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi : Keamanan Informasi , Teknologi Informasi Dan Network (Literature Review Sim)," *J. Ekon. Manaj. Sist. Inf.*, vol. Vol. 3, no. No. 5, pp. 564–573, 2022.

[8] A. Poeja Kehista *et al.*, "Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review)," *Jimt*, vol. 4, no. 5, pp. 625–632, 2023.

[9] P. Sundari and W. 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, doi: 10.31937/si.v12i1.1701.

[10] 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)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 5, pp. 1490–1498, 2020.

[11] V. I. Sugara, H. Syahrial, and M. Syafrullah, "Sistem Pemeriksa Keamanan Informasi Menggunakan National Institute of Standards and Technology (Nist) Cybersecurity Framework," *Komputasi J. Ilm. Ilmu Komput. dan Mat.*, vol. 16, no. 1, pp. 203–212, 2019, doi: 10.33751/komputasi.v16i1.1591.

[12] D. I. Khamil, "Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 dan ISO/IEC 27001:2013 (Studi Kasus : Diskominfo Kabupaten Gianyar)," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 3, pp. 1948–1960, 2022, doi: 10.35957/jatisi.v9i3.2310.

[13] T. E. Wijatmoko, "Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Pada Kantor Wilayah Kementerian Hukum Dan Ham Diy," *Cyber Secur. dan Forensik Digit.*, vol. 3, no. 1, pp. 1–6, 2020, doi: 10.14421/csecurity.2020.3.1.1951.

[14] I. Afrianto, T. Suryana, and S. Sufa'atin, "Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI - SNI ISO/IEC

27001:2009," *J. Ultim. InfoSys*, vol. 6, no. 1, pp. 43–49, 2015, doi: 10.31937/si.v6i1.278.

[15] M. Y. Putra and D. Tjahjadi, "Evaluasi Keamanan Informasi Pada Perguruan Tinggi Bina Insani Berdasarkan Indeks Keamanan Informasi SNI ISO/IEC 27001," *PIKSEL Penelit. Ilmu Komput. Sist. Embed. Log.*, vol. 6, no. 1, pp. 95–104, 2018, doi: 10.33558/piksel.v6i1.1404.