


Information Security Measurement using INDEX KAMI at Metro City

Ratna Savitri¹, Firmansyah², Dworo³, Muhammad Said Hasibuan^{4,*} 

^{1,2,3,4} *Institute Informatics and Business Darmajaya, Bandar Lampung 35136, Indonesia*

(Received: November 27, 2023; Revised: December 13, 2023; Accepted: January 15, 2024; Available online: January 29, 2024)

Abstract

Information security is a crucial issue that affects the overall business process, therefore it must be protected and secured. This research was conducted to assess the information security risks at Metro City Communication and Information Office in a structured manner towards information assets in identifying efforts to reduce risks as part of the information security management program. The research method begins with defining the scope, collecting data and supporting documents, evaluating the Information Security Index (KAMI), determining scores in 7 security areas, where strengths/maturity and weaknesses/deficiencies will be identified in each security area. Finally, after obtaining the evaluation results, recommendations will be made. The Information Security Index (KAMI) is a computer-based tool in excel format that can assess and evaluate the completeness and maturity level of information security implementation based on the SNI ISO/IEC 27001 criteria that describe the readiness of the information security framework. The data obtained by the researcher is based on interview results, examination of the availability of Information Security Management System (SMKI) documents, and evidence of SMKI implementation records/archives. The dashboard evaluation results for electronic system category score 17, which is in the high category, governance score is 69, risk management score is 29, framework score is 33, information asset management score is 69, technology score is 81 and supplement score is 0%. Based on verification of the results of the KAMI Index version 4.2 assessment file, a score of 275 was obtained, indicating that information security.

Keywords: INDEX KAMI, Information, Security

1. Introduction

Business practices in the cyber era have made information security a crucial issue that affects the entire business process, making information an important asset that must be protected and secured. Improving big data security management is a crucial step to ensure national security, promote stable community development, and protect public interests [1]. In the implementation of government IT management, protecting assets from harm is essential [2]. Information security challenges for organizations include confidentiality, integrity, and availability factors [3]. The Electronic-Based Government System is implemented with a continuous improvement principle in accordance with its development [4]. The management of electronic-based government system security is carried out in various processes to implement effective, efficient, and sustainable electronic-based government system protection and support quality electronic-based government services [5].

G. J. Simons' opinion on information security is that it is an effort to prevent fraud or detect fraud in a data-based system where the information is not physical [6]. There are three layers of security issues at each level, namely strategic, which refers to issues that have an impact on organizational strategy, tactical, which refers to the methodology issues implemented by the organization in managing security, and operational, which refers to the operation of security tools and actions [7]. The ISO/IEC 27001:2013 standard was reviewed and confirmed in 2019, and therefore this version remains current [8]. The ISO standard is based on a risk-based approach, process-oriented, and a sustainable improvement logic based on the plan-do-check-act (PDCA) approach. With a structured approach, ISO/IEC 27001 introduces standards and specifies requirements for preparing and implementing the ISMS along with a checklist [9]. This standard provides provisions for determining, implementing, maintaining, and continuously improving the Information Security Management System (ISMS) of an organization, including measuring and general security hazard

*Corresponding author: Muhammad Said Hasibuan (msaid@ darmajaya.ac.id)

 DOI: <https://doi.org/10.47738/jads.v5i1.152>

This is an open access article under the CC-BY license (<https://creativecommons.org/licenses/by/4.0/>).

© Authors retain all copyrights

requirements tailored to the interests of the organization [10]. SNI ISO/IEC 27001:2013 regulates all activities in controlling information security targets covering 14 security areas [11].

Previous studies have shown that risk control with the ISO 27002:2013 code of practice for information security controls can increase the cyber maturity value of an organization from a maturity value of 3.19 to 4.06 by implementing 12 new security controls. At maturity level 4, the organization ensures that cyber security management is managed, regulated, regularly reviewed, and continuous [12][13]. Research in Rembang Regency provides recommendations for risk mitigation efforts on 13 ISO 27001 controls based on equivalent risk analysis [14][15]. The results of the KAMI Index evaluation in a study in Sidoarjo Regency still need improvement to achieve ISO27001 certification [16][17]. Information security evaluations for an agency/organization are conducted every semester to achieve information security readiness and maturity level up to stage III+ [18][19].

The Head of Metro City Diskominfo has established an information security program as part of management responsibility, including the establishment of information security policies. One of the ways to prove this is through the implementation of information security programs in ITSP or related project initiatives. This study was conducted to assess the implementation of information security risks in order to identify mitigation measures that improve information security, the availability of information security procedures, and reduce information security risks. KAMI Index version 4.2 is a software in the form of an excel file formula to assess the readiness level based on SNI ISO/IEC 27001 provisions [20]). The results of the KAMI Index study serve as a basis for decision-making by the leadership in implementing government information security in Metro City.

2. Literature Review

2.1. Information Security Management System (ISMS)

ISMS is a comprehensive framework designed to establish, implement, operate, monitor, review, maintain, and improve information security within an organization. It encompasses a systematic approach to managing sensitive information, ensuring its confidentiality, integrity, and availability. The core objective of ISMS is to provide a structured methodology for identifying, assessing, and mitigating information security risks while promoting continual improvement. This system acts as a safeguard, recognizing the critical role that information plays in contemporary business practices, particularly in the cyber era where digital data is vulnerable to various threats.

One of the prominent standards guiding ISMS implementation is ISO/IEC 27001:2013. This internationally recognized standard sets forth requirements and guidelines for establishing, implementing, maintaining, and continually improving an organization's ISMS. ISO/IEC 27001 adopts a risk-based approach, emphasizing the identification and management of information security risks through a structured process. The Plan-Do-Check-Act (PDCA) cycle is integral to ISO/IEC 27001, providing a systematic and iterative framework for organizations to manage and enhance their information security posture.

ISMS addresses various security challenges faced by organizations, including confidentiality, integrity, and availability factors. By implementing ISMS, organizations can proactively address these challenges and establish a robust foundation for protecting their information assets. Additionally, ISMS facilitates compliance with legal, regulatory, and contractual requirements related to information security, enhancing the organization's overall governance and risk management practices.

In the context of the discussed research, the emphasis on ISMS, particularly through the lens of ISO/IEC 27001:2013, underscores the commitment to a structured and standardized approach to information security. The study assesses the implementation of ISMS in the government information security program in Metro City, using tools such as the KAMI Index to evaluate readiness based on SNI ISO/IEC 27001 provisions. This highlights the practical application of ISMS in real-world scenarios, showcasing its relevance in enhancing information security practices at both organizational and governmental levels. Overall, ISMS plays a pivotal role in ensuring the resilience and sustainability of information security measures in the face of evolving cyber threats.

2.2. ISO/IEC 27001:2013

ISO/IEC 27001:2013, often referred to as ISO 27001, is an international standard that provides a systematic and risk-based approach to managing information security within an organization. Published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO 27001 outlines the requirements for establishing, implementing, maintaining, and continually improving an ISMS. The standard is designed to be adaptable to various organizational structures, sizes, and industries, reflecting the universal importance of information security in the digital age.

One of the key features of ISO 27001 is its risk-based approach to information security. The standard emphasizes the identification, assessment, and treatment of information security risks, aligning with the organization's business objectives. This approach allows organizations to tailor their security measures based on their specific risk landscape, ensuring that resources are allocated efficiently to address the most significant threats.

ISO/IEC 27001:2013 follows the PDCA cycle, a management model that provides a structured and continuous framework for organizations to manage their ISMS effectively. This cycle involves planning and establishing the ISMS (Plan), implementing and operating the security controls (Do), monitoring and reviewing the system's performance (Check), and continually improving the ISMS based on the results of reviews (Act). This iterative process aligns with the dynamic nature of information security, allowing organizations to adapt and respond to emerging threats and vulnerabilities.

The standard covers a wide range of information security aspects, including organizational context, leadership and support, risk management, communication, and continual improvement. ISO 27001 certification demonstrates that an organization has implemented a robust ISMS and complies with international best practices in information security management.

In the context of the provided research, ISO/IEC 27001:2013 serves as a critical framework for evaluating and enhancing the government information security program in Metro City. The research incorporates the principles and provisions of ISO 27001, utilizing tools like the KAMI Index to assess the readiness level based on the standard's requirements. By aligning with ISO 27001, the government aims to ensure a systematic, risk-based, and internationally recognized approach to information security, fostering resilience against cyber threats and promoting a culture of continuous improvement in safeguarding sensitive information.

2.3. Cybersecurity Maturity

Cybersecurity maturity refers to the level of effectiveness and sophistication an organization has achieved in managing and mitigating cybersecurity risks. It encompasses the organization's ability to protect its information systems, data, and assets from cyber threats, adapt to evolving security challenges, and continuously improve its cybersecurity capabilities. Achieving a high level of cybersecurity maturity is crucial in today's digital landscape, where cyber threats are dynamic, sophisticated, and ever-present. A mature cybersecurity posture involves several key elements:

- 1) **Risk Management:** Mature organizations have a well-defined and proactive approach to identifying, assessing, and managing cybersecurity risks. This includes understanding the threat landscape, evaluating vulnerabilities, and implementing strategies to mitigate risks effectively.
- 2) **Governance and Leadership:** Strong cybersecurity maturity is often associated with effective governance and leadership. This includes having a clear understanding of the organization's risk appetite, establishing policies and procedures, and ensuring that leadership is actively involved in cybersecurity decision-making.
- 3) **Security Awareness and Training:** Organizations with high cybersecurity maturity prioritize employee awareness and training programs. This ensures that all members of the organization understand their roles and responsibilities in maintaining security, reducing the risk of human error that can lead to security incidents.
- 4) **Incident Response and Recovery:** Mature organizations have well-defined incident response plans in place. This involves the ability to detect and respond to security incidents promptly, minimizing the impact and facilitating a quick recovery.
- 5) **Continuous Monitoring and Improvement:** Cybersecurity maturity is an ongoing process that requires continuous monitoring of the security landscape and regular assessments of the effectiveness of security controls. Mature

organizations are committed to a cycle of continuous improvement, adapting their security measures to address emerging threats.

In the context of the provided research, the concept of cybersecurity maturity is likely relevant to assess the government information security program in Metro City. The research may investigate how well the organization has progressed in terms of building and enhancing its cybersecurity capabilities, implementing best practices, and adapting to the evolving threat landscape. Evaluating cybersecurity maturity allows organizations to identify areas for improvement and prioritize investments in security measures that align with their overall risk management strategy.

The research may also consider frameworks and models, such as the Capability Maturity Model Integration (CMMI) for cybersecurity, to provide a structured approach to assessing and improving cybersecurity maturity levels. This ensures that the organization moves towards a more resilient and mature cybersecurity posture, addressing the challenges posed by an increasingly complex and dynamic cybersecurity landscape.

3. Methodology

3.1. Research Framework

The researcher created a systematic, directed, and organized framework for research stages as a reference to reach the final stage. The research steps can be seen in Figure 1.

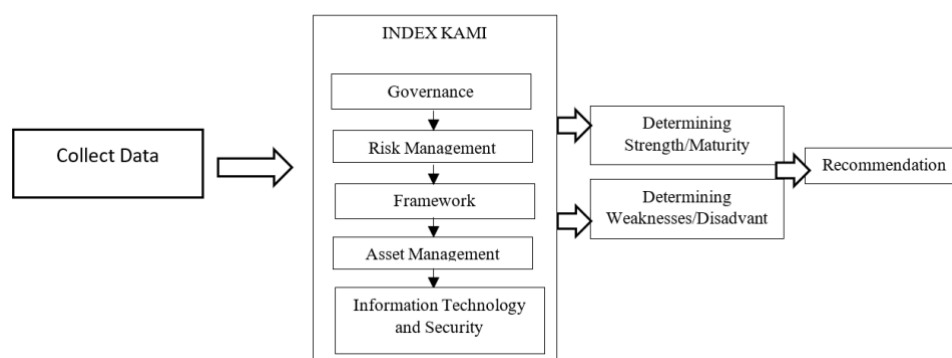


Figure 1. Research framework

3.2. Data Collection and Supporting Evidence

The researcher collects data and supporting evidence through the following methods:

- 1) Interviewing sources from the Metro City Information and Communication Office (Diskominfo).
- 2) Examining the ISMS documents according to the availability checklist status such as policy documents, objectives, plans, standards, and procedures/guidelines.
- 3) Examining evidence (record/archives) of ISMS implementation.

The collected data will be used in the evaluation of the KAMI index to provide an overview of the applied information security, determine strengths/maturity and weaknesses/shortcomings, and develop improvement recommendations and prioritize them.

3.3. Evaluation Model

Based on the standard requirements of SNI ISO/IEC 27001, BSSN established an evaluation model for measuring information security readiness using the KAMI index version 4.2. The evaluation is carried out by filling in the status columns of stages 1 to 3 in the 7 areas that are the objectives of information security implementation, with the discussion limit covering security aspects established by ISO/IEC 27001:2013 standard [21].

In the ES Category Score, a score value and category description will be obtained at a low, high, or strategic level. Then, the total evaluation value is obtained from each score of the 7 areas and maturity level along with the status. The total evaluation value shows the completeness level of ISO27001 standard implementation according to the ES category indicator color as shown in the KAMI index version 4.2 assessment result dashboard in figure 2.

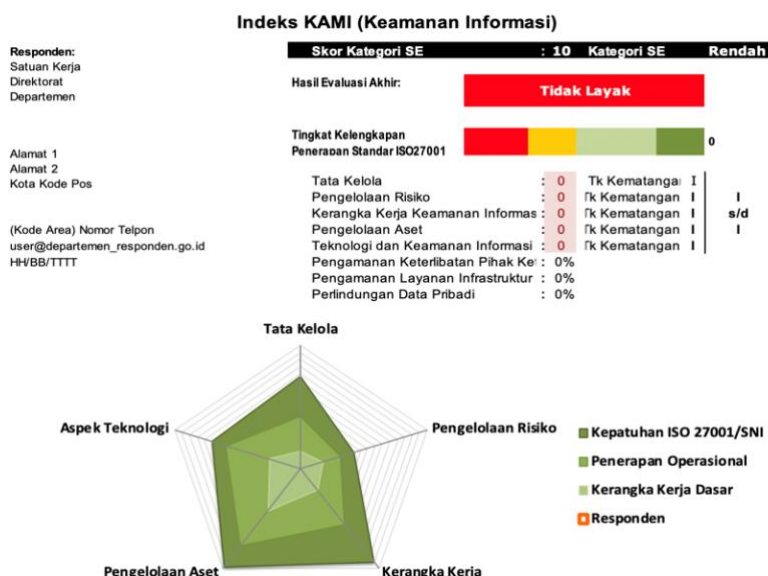


Figure 2. KAMI index version 4.2 dashboard

In the assessment process, the score is measured through the value score of questions in 7 sections, namely electronic systems category, governance, risk, framework, asset management, technology, and supplements. Each security section has 4 different security statuses according to the defined question stage in table 1.

Table 1. Category Status and Security

Security Status	Security Category		
	1	2	3
Not implemented	0	0	0
In planning	1	2	3
In implementation/Partially implemented	2	4	6
Fully implemented	3	6	9

Based on the KAMI index diagram results, it can be seen that there is a need for improvement and alignment between various information security sections. The relationship between the electronic systems category and readiness status can be seen in table 2.

Table 2. Correlation of ES Category Scores and Readiness Status

Electronic Systems Category				
10	15	<i>Skor akhir</i>		Readiness Status
		0	174	Not eligible
		175	312	Basic framework fulfillment
		313	535	Adequate
		536	645	Good
16	34	<i>Skor akhir</i>		Readiness Status
		0	174	Not eligible
		175	312	Basic framework fulfillment
		313	535	Adequate
		536	645	Good
35	50	<i>Skor akhir</i>		Readiness Status
		0	174	Not eligible
		175	312	Basic framework fulfillment
		313	535	Adequate
		536	645	Good

The maturity of the KAMI index is defined in 5 levels, with level I at the initial stage, level II at the basic framework implementation stage, level III already defined and consistent, level IV already managed and measured, and level V at the optimal maturity stage. In addition, there are detailed levels between -I+, II+, III+, and IV+. The minimum maturity compliance for ISO/IEC 27001:2013 standard certification is level III+.

After all sections in the KAMI index are completed, the strengths and maturity of each security area are obtained. Each strength/maturity can be described in detail as a report to the management on the readiness level of the agency in terms of completeness and security maturity. Based on the achieved strength/maturity level, weaknesses in each security area will be identified. Each weakness/shortcoming will be described in detail as a report to the management. Weaknesses/shortcomings will be considered by the management for decision making.

3.4. Recommendation

Based on the evaluation results, strengths/maturity, weaknesses/shortcomings, it is concluded that the level of readiness and maturity of information security requires appropriate recommendations in areas that need improvement and enhancement towards information security readiness. Implementing recommendations will increase the value of our KAMI index in the next evaluation period, which means an improvement in the availability and sufficiency of information security.

4. Result and Discussion

4.1. Research Object Scope

The research object of this study is the Metro City Communication and Information Office with research locations at the headquarters, data center, and disaster recovery center (DRC) located in one office building area. The research scope is as shown in table 3.

Table 3. Research Object Scope

Scope	Description
Research Location	Headquarters, data center, and disaster recovery center.
Public Services Managed	Infrastructure services (Data Center, NOC, Network, Server) and 79 Information System Applications.
Critical IT Assets	Government employee data information of Metro City, applications with high ES category value and the website of Metro City Government, internal Regional Device Organization application server and backup hosting server exabytes for PLIH and JDIH along with network infrastructure assets.
Data center	Located in a special room (server room managed internally), the data center is located in PDNS with backup (mirroring) at the Metro City Communication and Information Office used for managing applications in the scope of the Metro City Regional Device.
Disaster recovery center	Managed internally and applies the data center backup concept for backup services of application databases.

4.2. Data and Supporting Evidence Collection

Data and supporting documents were collected based on the availability checklist of ISMS documents as shown in table 4.

Table 4. ISMS Document Availability Checklist

No	Document Name	Yes	No	Description (D:Draft, R:Released, T:Socialized)
Policies, Objectives, Plans, Standards				
1	Information security policy	Yes		R, SPBE Regional Regulation
2	Organization, roles, and responsibilities for information security	Yes		R, Regional Device Regulation
3			No	
4	ICT risk management policy	Yes		R, Head of Communication and Information Office Decree Risk Management
5	Business continuity management framework		No	
6	Policy for the use of ICT resources		No	
Procedures/Guidelines:				
1	Document control		No	
2	Record control		No	
3	ISMS internal audit		No	
4	Corrective and preventive actions		No	
5	Labeling, securing, exchanging, and disposing of information		No	
6	Removable media management and disposal		No	
7	Monitoring the use of ICT facilities		No	
8	User access management		No	
9	Teleworking		No	
10	Control of software installation and intellectual property rights (IPR)		No	
11	ICT change management		No	
12	Management and reporting of information security incidents		No	

In the availability status table of ISMS documents and the information security system framework, it is shown that the institution has issued an information security policy, information security roles and responsibilities, and ICT risk management policy but has not yet been socialized. Meanwhile, not all procedures/guidelines are available in accordance with ISMS.

This activity was carried out in line with the interview process in a meeting attended by the Head of Information Technology Division, Information and Cryptography Functional Officer, Data Center Infrastructure Functional Officer, and Network Infrastructure Functional Officer. Supporting evidence (records/archives) of ISMS implementation includes Socialization Photos, internet network user screenshots, application screenshots, and Employee Competency Improvement Program Certificates.

4.3. Electronic System Category Evaluation

The ES category area assesses the electronic systems used, equipped with documents and document numbers. The assessment consists of 10 questions, with a Low-C score of 1, High-B score of 2, and Strategic-A score of 5. The Electronic System Category score is determined by the sum of all scores on the 10 questions.

From the 10 questions, it is found that only 1 statement has a strategic status, which is the use of special cryptography techniques certified by the State. 2 statements do not have documents, namely related to investment value and data classification/criticality level. The installed assets owned are worth less than 3 billion for accommodating the implementation of the agency's functions with a small workload. Supporting asset documents are not owned by the

agency but are recorded in the Metro City Regional Financial and Asset Management Agency (BPKAD) Asset Division. The Metro City Communication and Information Office manages Electronic Systems in the high category with a score of 17 (table 2).

4.4. Information Security Completeness and Maturity Evaluation

The evaluation of information security completeness and maturity is divided into 5 parts, namely governance, risk, framework, asset management, and technology. In each section, the status column is filled in accordance with the implementation of information security with the determination of scores from stage 1 to stage 3 according to table 5.

Table 5. Maturity Level Scores Application Status Score Determination

Application Status	Score Determination		
	1	2	3
Not implemented	0	0	0
In planning	1	2	3
In implementation/partially implemented	2	4	6

4.5. Information Security Governance

The governance area assesses the readiness of information security governance along with the functions/duties/responsibilities of security managers. There are 3 questions with a planning status supported by planning evidence documents. The final score of Metro City Communication and Information Office is 69, with implementation stages 1 & 2 worth 48, so the status of the assessment for stage 3 implementation is declared valid. The validity and status of the question results at maturity level II in stage II are Yes. Meanwhile, the validity and status of the question results at maturity level III and maturity level IV are No because there are maturity level III and IV questions that have answers with a Not Implemented security status with a score of 0, according to the evaluation results in table 6.

Table 6. Information Governance Evaluation Scores

Description	Result
Total Information Governance Evaluation Score	69
Total Stage 1 & 2 Implementation Scores	48
Stage 3 Implementation Assessment Status	Valid
Maturity Level II Score Status	II
Maturity Level III Score Status	No
Maturity Level IV Score Status	No

After the evaluation, one of the strengths is that all information security implementers involved in Metro City Communication and Information Office already have sufficient skills and abilities to meet the established requirements, especially in terms of technical and operational control aspects of information security. Any information security issues that arise have been considered as part of the process of supporting strategic decisions in taking necessary corrective actions to improve the effectiveness of information security control implementation.

One of the weaknesses is that not all roles of information security implementers have been mapped to the overall information security program needs, such as the need for audits in the organization and conditioning the separation of authorities for implemented security controls

4.6. Information Security Risk Management

The risk area evaluates the readiness of information security risk management implementation as a basis for implementing information security strategies. The total evaluation score for this area is 23, with a total stage 1 & 2 implementation score of 23, which is less than the minimum score limit for stage 3 implementation, which is 36, so the status of the assessment for stage 3 implementation is declared invalid. The maturity level II score status is I+. Meanwhile, the validity and status of the question results at maturity level III, maturity level IV, and maturity level V are No because there is maturity level III, IV, and IV questions that have answers with a Not Implemented security status with a score of 0, according to the evaluation results in table 7.

Table 7. Information Security Risk Management Evaluation Scores

Description	Result
Total Information Security Risk Management Evaluation Score	23
Minimum Score Limit for Stage 3 Implementation Score	36
Total Stage 1 & 2 Implementation Scores	23
Stage 3 Implementation Assessment Status	Invalid
Maturity Level II Score Status	I+
Maturity Level III Score Status	No
Maturity Level IV Score Status	No
Maturity Level V Score Status	No

After the evaluation, one of the strengths is that the minimum risk level that is understood has been established by the management of Metro City Communication and Information Office in order to evaluate the analyzed risk levels. In the process of managing risk management related to ownership rights and information asset management providers that exist, it has not been clearly defined in the methodology documents, including critical assets and their work processes that utilize these assets.

One of the weaknesses is that the information security risk management roadmap has not been adequately documented and implemented in the risk assessment and evaluation process. The mitigation steps and risk management measures currently have not been systematically and adequately developed.

4.7. Information Security Management Framework

The assessment in this area aims to review the completeness and readiness of the information security management framework, including policies and procedures related to information security management and their implementation strategies. The questions consist of 2 groups. The total evaluation score for the framework is 33, with a total stage 1 & 2 implementation score of 33, which is less than the minimum score limit for stage 3 implementation, which is 64, so the status of the assessment for stage 3 implementation is declared invalid. The maturity level II score status is I+. Meanwhile, the validity and status of the question results at maturity level III, maturity level IV, and maturity level V are No because there is maturity level III, IV, and IV questions that have answers with a Not Implemented security status with a score of 0, according to the evaluation results in table 8.

Table 8. Information Security Management Framework

Description	Result
Total Information Security Management Framework Evaluation Score	33
Minimum Score Limit for Stage 3 Implementation Score	64
Total Stage 1 & 2 Implementation Scores	33
Stage 3 Implementation Assessment Status	Invalid
Maturity Level II Score Status	I+
Maturity Level III Score Status	No

One of the strengths in this area is that there is a process to recognize situations that are vulnerable to information security and determine them as incidents to be addressed according to applicable procedures, and information security implementation plans have been concretely realized.

One of the weaknesses is that the planning for the utilization of information security technology, whose implementation and updates are adjusted to different needs and various risk threats, has been identified but has not been officially formulated and established even though some aspects have been realized.

4.8. Information Asset Management

The purpose of the assessment is to review the completeness of information asset security, including the entire range of asset utilization. The questions are divided into 2 groups: information asset management and physical security. The total evaluation score for information asset management is 69, with a total stage 1 & 2 implementation score of 69, which is less than the minimum score limit for stage 3 implementation, which is 88, so the status of the assessment for stage 3 implementation is declared invalid. The maturity level II score status is I+. Meanwhile, the validity and status

of the question results at maturity level III are No because there are maturity level III questions that have answers with a Not Implemented security status with a score of 0, according to the evaluation results in table 9.

Table 9. Information Asset Management Evaluation Scores

Description	Result
Total Information Asset Management Evaluation Score	69
Minimum Score Limit for Stage 3 Implementation Score	88
Total Stage 1 & 2 Implementation Scores	69
Stage 3 Implementation Assessment Status	Invalid
Maturity Level II Score Status	I+
Maturity Level III Score Status	No

One of the strengths in this area is that some threat mitigation measures are already available, such as rules regarding software installation on IT assets but have not been documented. The background check process for human resources is already in place.

One of the weaknesses is that there is no procedure regarding the backup process, and there is no mechanism for testing data restoration. There is no regulation for securing agency-owned computing devices when there is a task requirement outside the official work location.

4.9. Technology and Information Security

The purpose of the assessment is to evaluate the completeness, consistency, and effectiveness of technology use in securing information assets. The total evaluation score for Technology and Information Security is 81, with a total stage 1 & 2 implementation score of 69, which is greater than the minimum score limit for stage 3 implementation, which is 68, so the status of the assessment for stage 3 implementation is declared valid. The result status at maturity level II in stage II is shown in table 10.

Table 10. Technology and Information Security Evaluation Scores

Description	Result
Total Technology and Information Security Evaluation	81
Minimum Score Limit for Stage 3 Implementation Score	68
Total Stage 1 & 2 Implementation Scores	69
Stage 3 Implementation Assessment Status	Valid
Maturity Level II Score Status	II
Maturity Level III Score Status	No
Maturity Level IV Score Status	No

One of the strengths in this area is that the Metro City Communication and Informatics Office has implemented encryption to protect critical data assets in accordance with applicable management policies. The Metro City Communication and Informatics Office has established provisions for implementing encryption but has not yet been included in procedures/policies.

From the evaluation results, one of the weaknesses is that only some desktops and servers have the latest operating system updates, and not all clients and servers are protected from virus (malware) attacks.

4.10. Supplementary Evaluation

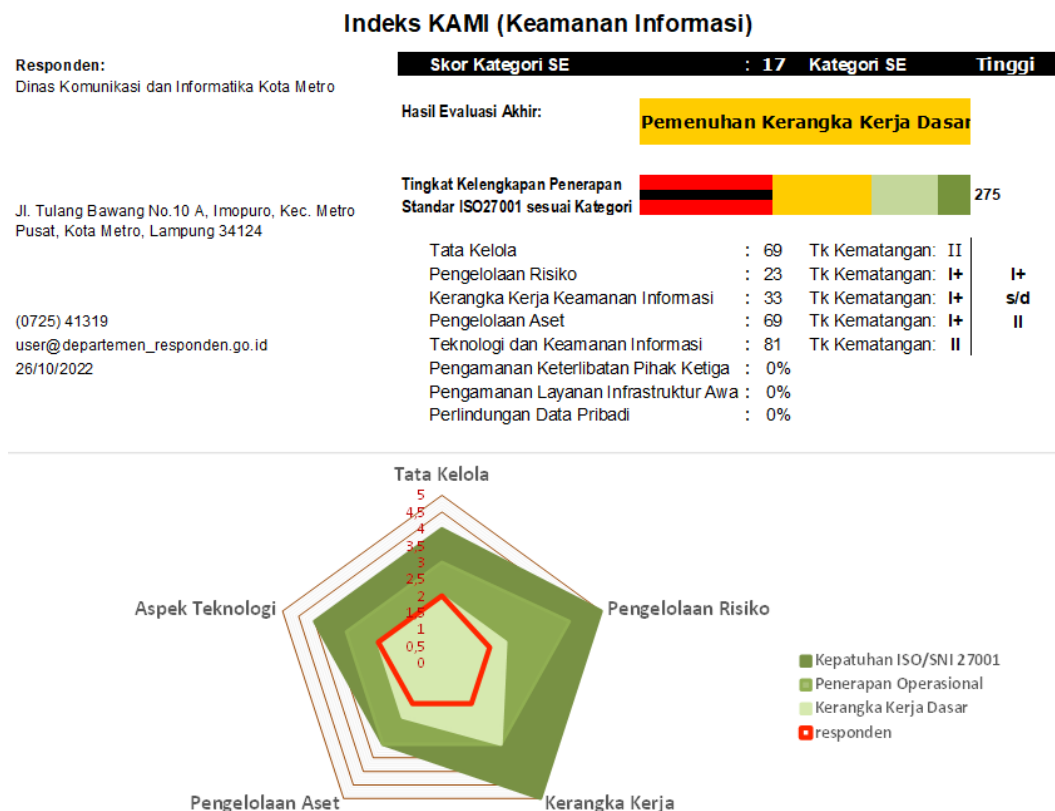
The supplementary area aims to assess the completeness, consistency, and effectiveness of technology use, which is divided into 3 groups of questions: third-party service provider involvement security, cloud service infrastructure security, and personal data protection. The evaluation score obtained by the Metro City Communication and Informatics Office for the supplementary evaluation is 0 for all question groups because this area has not been implemented, so no strengths or weaknesses are obtained for the supplementary area, as shown in table 11.

Table 11. Supplementary Evaluation Score

Description	Result
Third-Party Service Provider Involvement Security	0
Third-Party Risk Management and Security Management	0
Subcontractor/Outsourcing Management for Third Parties	0
Third-Party Service and Security Management	0
Third-Party Service Change Management and Policies	0
Asset Handling	0
Third-Party Incident Management	0
Third-Party Service Continuity Plan	0
Cloud Service Infrastructure Security	0
Personal Data Protection	0

4.11. KAMI Index Dashboard Version 4.2

As expected, as stated in the "Introduction" chapter can ultimately result in "Results and Discussion" chapter, so there is compatibility. Moreover, it can also be added the prospect of the development of research results and application prospects of further studies into the next (based on result and discussion).



5. Conclusion

Upon verification of the KAMI Index version 4.2 assessment file results, key conclusions about the information security readiness of Metro City Communication and Informatics Office have been drawn. The office manages Electronic Systems at a high category, achieving a final evaluation score that meets the basic framework of ISO 27001 standards with a completeness level, as indicated by a score of 275. This suggests that the information security readiness status is positioned between the stages of meeting the basic framework with maturity levels of I+ to II. However, the verification process in the Supplementary Area was hindered by incomplete supporting data presented by the office, necessitating future assessments in this area.

In light of the findings, recommendations for improvements have been identified. These include the development of more detailed technical guidelines for managing Electronic Systems with the involvement of all stakeholders, the creation of information security risk management guidelines accompanied by an updated and periodically reviewed risk register, and the establishment of rules and implementations pertaining to personal data usage, including written authorization by data owners. Additionally, the office is advised to promptly define information asset separation in accordance with applicable legislation, formalize a list of necessary information backups based on criticality levels, tighten network segmentation for enhanced logical security, and initiate a formal program for monitoring and evaluating application security independently. Furthermore, the allocation of licenses for Electronic Systems, implementation and legalization of procedures related to information security, and regular KAMI Index evaluations are recommended. Looking ahead, the next evaluation should include the completion of the supplementary section to gauge compliance, consolidate actions, and assess the successful use of technology in information security.

6. Declarations

6.1. Author Contributions

Conceptualization: R.S., R.S; Methodology: R.S.; Software: F.; Validation: F., R.S.; Formal Analysis: F., D; Investigation: D.; Resources: M.S.H.; Data Curation: D.; Writing Original Draft Preparation: D. and M.S.H.; Writing Review and Editing: D. and M.S.H.; Visualization: M.S.H.; All authors have read and agreed to the published version of the manuscript.

6.2. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

6.3. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

6.4. Institutional Review Board Statement

Not applicable.

6.5. Informed Consent Statement

Not applicable.

6.6. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

- [1] M. Yang, "Information security risk management model for big data," *Advances in Multimedia*, vol. 2022, no. august, pp. 1–10, 2022. doi:10.1155/2022/3383251.
- [2] I. P. Syahindra, C. Hetty Primasari, and A. Bagus Pradipta Iriantor, "Evaluasi Risiko Keamanan informasi DISKOMINFO provinsi XYZ Menggunakan indeks Kami Dan ISO 27005 : 2011," *J. Teknoinfo*, vol. 16, no. 2, pp. 165–182, 2022. doi:10.33365/jti.v16i2.1246.
- [3] S. Nurul, S. Anggrainy, and S. Aprelyani, "Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan INFORMASI, Teknologi Informasi Dan Network (literature review sim)," *Jurnal Ekonomi Manajemen Sistem Informasi*, vol. 3, no. 5, pp. 564–573, 2022. doi:10.31933/jemsi.v3i5.992.
- [4] "Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik." 2018.
- [5] "Peraturan Badan Siber Dan Sandi Negara Nomor 4 Tahun 2021 Tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Dan Standar Teknis Dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik." 2021.
- [6] A. Hartomo, "Perencanaan Strategis Sistem Informasi Dan Sistem Manajemen Keamanan informasi berbasis ISO / IEC

- 27001 : 2013 Menggunakan Ward & Peppard Pada Perusahaan transshipment,” *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 10, no. 1, pp. 141–154, 2023. doi:10.25126/jtiik.20231015604.
- [7] P. Belsis, S. Kokolakis, and E. Kiountouzis, “Information Systems Security from a Knowledge Management Perspective,” *Information Management and Computer Security*, vol. 13, no. 3, pp. 189–202, 2005. doi:10.1108/09685220510602013.
- [8] M. Mirtsch, J. Kinne, dan K. Blind, “Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis,” *IEEE Trans. Eng. Manag.*, vol. 68 No.1, no. 1, pp. 87–100, Feb 2021.
- [9] M. Podrecca dan M. Sartor, “Forecasting the diffusion of ISO/IEC 27001: a Grey model approach,” *Total Qual. Manag.*, vol. 35, no. 9, pp. 123–151, Feb 2023, doi: 10.1108/TQM-07-2022-0220.
- [10] [1] A. A. Putra, O. D. Nurhayati, and I. P. Windasari, “Perencanaan Dan Implementasi information security management system MENGGUNAKAN framework ISO/IEC 20071,” *Jurnal Teknologi dan Sistem Komputer*, vol. 4, no. 1, pp. 60–72, 2016. doi:10.14710/jtsiskom.4.1.2016.60-66.
- [11] M. Bakri dan N. Irmayana, “Analisis dan Penerapan Sistem Manajemen Keamanan Informasi SIMHP BPKP Menggunakan Standar ISO 27001,” *J. TEKNOKOMPAK*, vol. 11 No.2, pp. 41–44, 2017, doi: <https://doi.org/10.33365/jtk.v11i2.162>.
- [12] E. J. Wibowo dan K. Ramli, “Impact of Implementation of Information Security Risk Management and Security Controls on Cyber Security Maturity (A Case Study at Data Management Applications of XYZ Institute),” *J. Sist. Inf.*, vol. 18 No. 2 (2022), no. 2, PP. 1-17, Oktober 2022, doi: <https://doi.org/10.21609/jsi.v18i2.1146>.
- [13] H. Wang and P. Budsaratagoon, “Exploration of an “Internet+” Grounded Approach for Establishing a Model for Evaluating Financial Management Risks in Enterprises”, *Int. J. Appl. Inf. Manag.*, vol. 3, no. 3, pp. 109–117, Sep. 2023.
- [14] F. Anindhita, Suprpto, dan A. R. Perdanakusuma, “Perencanaan Pengelolaan Keamanan Informasi Berbasis ISO 27001 menggunakan Indeks KAMI Studi Kasus: Dinas Komunikasi dan Informatika Kabupaten Rembang,” *J. Pengemb. Teknol. Inf. Dan Ilmu Komput.*, vol. 3 No. 6, Juni 2019, pp. 6009–6015, Jun 2019.
- [15] F. Ali Faraj Alyaqobi and N. Adnan Bin Yahaya, “A Systematic Review on Image Data Protection Methods,” *Int. J. Informatics Inf. Syst.*, vol. 5, no. 3, pp. 131–141, Sep. 2022
- [16] N. Arman, W. H. Nugraha Putra, dan A. Rachmadi, “Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo menggunakan Indeks Keamanan Informasi (KAMI),” *J. Pengemb. Teknol. Inf. Dan Ilmu Komput.*, vol. 3, No.6, Juni 2019, pp. 5750–5755, Jun 2019.
- [17] Y. Shi, “Formulation and Implementation of a Bayesian Network-Based Model”, *Int. J. Appl. Inf. Manag.*, vol. 3, no. 3, pp. 101–108, Sep. 2023.
- [18] H. A. Pratiwi dan L. Wulandari, “Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor,” *JiEMAR*, vol. 2 No.5, pp. 146–163, 2021, doi: <https://doi.org/10.7777/jiemar>.
- [19] G. Lisanawati and J. E. Kehinde, “When Technology Meets Money Laundering, What Should Law Do? New Products and Payment Systems and Cross Border Courier,” *Int. J. Informatics Inf. Syst.*, vol. 5, no. 3, pp. 142–149, Sep. 2022
- [20] “Konsultasi dan Assessment Indeks KAMI,” BSSN, 2021. Accessed: May 14, 2023. [Online]. Available at: <https://bssn.go.id/index-kami/>
- [21] “Aplikasi Indeks Keamanan Informasi (Indeks KAMI) Versi 4.2.” BSSN, Mei 2021. Accessed: May 14, 2023. [Online]. Available at: <https://bssn.go.id/index-kami/>