BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **25**, No 2
Sofia • 2025 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2025-0018

Alignment of KAMI Index with Global Security Standards in Information Security Risk Maturity Evaluation

Aji Supriyanto, Arief Jananto, Jeffri Alfa Razaq, Budi Hartono, Fitri Damaryanti

Faculty of Information Technology and Industry, Universitas Stikubank, Semarang, Indonesia
E-mails: ajisup@edu.unisbank.ac.id ajananto@edu.unisbank.ac.id mrjf@edu.unisbank.ac.id budihartono@edu.unisbank.ac.id rr.fitri0038@mhs.unisbank.ac.id

Abstract**:** *Various incidents of information security breaches in Indonesia in 2024, especially in government agencies, are very dangerous. Even the Temporary National Data Center* (*PDNS*) *Surabaya was paralyzed in public services. One of the reasons is that adequate security standards have not been implemented, even though in Indonesia, there are already Information Security standards* (*KAMI Index*)*. This study aims to determine the alignment of the KAMI index with international security standards such as ISO 27001 and NIST based on the main security principles, namely Confidentiality, Integrity, Availability* (*CIA triad*)*. The method is mapping the alignment of control elements* (*domains*) *in the standard based on ontology. The results showed that the level of alignment reached 56 percent* (*56%*)*, or relatively high. This means harmonization regarding terminology, evaluation methods, and integration in national regulations is still needed to improve alignment with international standards.*

Keywords**:** *Alignment mapping, Information security, KAMI Index, ISO 27001, NIST.*

1. Introduction

Ensuring information security in an organization is crucial for protecting information assets and maintaining public trust**.** Nearly all private and government organizations have implemented some form of information security**,** yet security breaches continue to occur frequently. There are various challenges and obstacles in implementing national information security frameworks [1]. One of the major challenges faced by developing countries is the shortage of skilled cybersecurity professionals [2]. Cyberattacks, malicious activities, and fraud within information systems have evolved into a widespread global challenge**.** Cybersecurity**,** which focuses on protecting networks, systems, and data from information security threats, must ensure the Confidentiality, Integrity, and Availability (CIA Triad) of information [3].

A report by the Cybersecurity Research Institute (CISSReC) from bloombergtechnoz.com summarized seven major cyberattacks and data breaches that

occurred in Indonesia throughout 2024, targeting the state railway company (PT. KAI), the state railway company's General Election Commission (KPU), Digital infrastructure company (Biznet). Next, the State Civil Service Agency (BKN), National Data Center (PDN), the Tax Authority (NPWP), and online gambling platforms. The National Temporary Data Center (PDNS) in Surabaya was even rendered inoperable, disrupting public services. This situation arises due to the emergence of increasingly sophisticated cyber threats and attack models, while many security implementations remain simple, fragmented, and fail to meet established cybersecurity standards. Furthermore, the implementation of the Information Security Index (KAMI Index) Version 4.2 in Indonesia has not been fully optimized. This shows that the level of security maturity is still low. For instance Provincial Revenue Agency (BAPENDA) of Central Java: Security maturity Level I – I+ [4], Metro City: Level II [5], Ministry of Public Works and Public Housing (PUPR): Level I+ – II [6], PKU Muhammadiyah Hospital, Surakarta: Level I+ until II [7], BAKAMLA (Indonesian Maritime Security Agency): Level I – I+ [8]. Most organizations in Indonesia still operate at security maturity levels below Level III, which is lower than the required Level III+ as mandated by KAMI Index and ISO/IEC 27001 [5, 9, 10].

Many organizations have yet to implement security systems systematically and comprehensively. Meanwhile, various Information Security Management Systems (ISMS) have been developed globally, which should be adopted by both government and private organizations. Several internationally recognized security standards, such as ISO/IEC 27001, NIST, and COBIT, have been widely used and acknowledged at the global scale [11, 12]. On the other hand, at the national level, Indonesia has adopted the KAMI Index as its primary information security standard. The KAMI Index is based on ISO/IEC 27001 [13, 14]. Integrating international and national security standards is critical to ensure national organizations align with global security frameworks [15-17]. However, this integration requires harmonization of control elements across the adopted security standards [18].

Aligning national security standards with global best practices enhances organizational trust and credibility [17]. Organizational security requirements include developing and aligning international security standards, particularly ISO/IEC 27001:2013, which has been widely adopted [18]. Successful security standard alignment requires organizational readiness [18, 19], comprehensive training and awareness programs [20], and institutional capacity strengthening [17]. This process incurs significant costs, yet it is a necessary investment to protect critical information assets [21] and address modern IT security challenges [21]. Effective organizational information management is a fundamental component in achieving Good Corporate Governance (GCG) [11, 22]. The implementation of information security within an organization requires structured measures and controls to ensure the CIA of information [23]. Under ISO/IEC 27001, the risk management process focuses on: Establishing a risk assessment methodology, Identifying potential security risks, Conducting risk analysis and evaluation [24].

Cybersecurity standards represent best practices for information security, secure communication and are generally applicable across all sectors [25]. Each security

standard or framework has its strengths and weaknesses. In the context of security audits, collaboration and integration should be prioritized to mitigate individual shortcomings [16, 26]. The KAMI Index adopts the ISO/IEC 27001 standard, primarily due to its widespread adoption in the market and the increasing number of organizations obtaining certification [8, 29, 30]. A recommended approach for optimal collaboration and integration involves aligning with the National Institute of Standards and Technology (NIST), which guides security maturity levels [4, 31, 32]. While ISO/IEC 27001 offers a managerial framework, NIST provides technical guidelines [25].

This study is motivated by the fact that many government and private institutions have yet to implement information security systems with clear and standardized measurement frameworks, relying instead on subjective assessments. During this transition phase, the KAMI Index Version 4.2, which still adheres to ISO/IEC 27001:2013 before transitioning to a new standard, necessitates an alignment assessment for information security compliance. Therefore, this research aims to establish alignment among security control elements to evaluate information security risk maturity. The harmonization between ISO/IEC 27001:2013 and NIST is expected to enhance the national-scale KAMI Index, ensuring compliance with international standards. The adoption of these standards should be grounded in the implementation of fundamental security frameworks to uphold core security principles, particularly the CIA Triad [8, 10, 11].

This study aims to determine the alignment of the KAMI index with international security standards such as ISO 27001 and NIST based on the main security principles, namely Confidentiality, Integrity, Availability (CIA Triad). The method used is mapping the alignment of security standards through an ontology-based mapping model for assessing information security maturity. This alignment is crucial for facilitating implementation, evaluation, and serving as a foundational reference for transitioning to ISO/IEC 27001:2022. The findings of this research can be utilized as an alternative standard for assessing organizational security maturity in developing countries at both local and national scales, with international recognition.

2. Literature study

2.1. ISO/IEC 27001

ISO 27001 is part of the ISO/IEC 27000 standard, a series of numbered international information security standards jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The official title of the ISO 27001 standard is “Information Technology – Security Techniques – Information Security Management Systems – Requirements”, commonly referred to as ISO 27001 [11, 37]. This system focuses on risk management, defining procedures for detecting, assessing, and mitigating IT risks. ISO/IEC 27001 provides a standardized approach to information security management and establishes security controls, including access control, risk assessment, incident management, and business continuity[38]. The implementation

process of the ISMS based on ISO 27001 ensures information security through a risk-based approach [26, 33, 39].

ISO/IEC 27001 has been adopted by various organizations and enterprises worldwide [9]. It serves as a framework for identifying security failures, assessing the impact of information security threats, and determining the most effective controls to mitigate organisational risks [11]. One key aspect of ISO/IEC 27001 is its emphasis on structured incident response mechanisms[40]. The ISO/IEC 27001 standard comprises 21 mandatory requirements, including 7 core mandates and 14 security control categories, guiding the design and development of an ISMS policy. The SNI ISO/IEC 27001:2013 standard governs all security control objectives across 14 security domains (clauses) [10, 41]. These domains align with the security controls listed in Annex A, covering 34 security objectives and 114 ISMS controls [10, 21, 29].

The ISO/IEC 27001 standard mandates the establishment of a risk assessment framework that involves identifying, analyzing, and evaluating risks, and ultimately selecting a risk treatment plan. This process is essential in developing security controls to protect an organization's information assets [11]. Within an organizational context, ISO/IEC 27001:2013 serves as a structured standard outlining the requirements for establishing, implementing, maintaining, and continuously improving information security strategies. These prerequisites are critical to ensuring that information security risks are effectively mitigated, aligning with broader security strategies aimed at safeguarding the confidentiality of data through risk management processes. Risk analysis and interpretation are facilitated using risk assessment tools, which aid in systematically evaluating threats and vulnerabilities [42].

2.2. KAMI Index

In Indonesia, the Badan Sandi dan Siber Nasional (BSSN) (National Cyber and Crypto Agency) serves as the government institution responsible for issuing guidelines to evaluate and assess the readiness for Information Security (KAMI), which refers to the SNI ISO/IEC 27001 standard [8, 13]. The Keamanan Informasi (KAMI) Index, or simply KAMI Index, is an assessment tool used to determine the level of information security readiness within companies and institutions [8, 10]. Initially, the KAMI Index was developed by the Ministry of Communication and Informatics [10]. The index serves as a methodological tool for measuring an organization's preparedness in aligning with ISO/IEC 27001:2013 [4, 7]. According to the official BSSN website (**https://www.bssn.go.id/indeks-kami/**), the current KAMI Index version 4.2 is widely used across Indonesia and aligns with the National Standard of Indonesia (SNI) ISO/IEC 27001:2013. However, starting in October 2025**,** version 5.0 will be introduced, which aligns with SNI ISO/IEC 27001:2022.

The KAMI Index assesses several key aspects, including Governance, Framework, Asset Management, Third-Party Technology Aspects, Cloud Service Security, and Personal Data Protection (PDP). The evaluation framework using the KAMI Index covers seven main domains, which include: (a) Electronic system categorization; (b) Information security governance; (c) Information security risk

management; (d) Information security management framework; (e) Information asset management; (f) Information technology and security; (g) Supplementary measures [7, 8, 10]. The Supplementary Measures category refers to additional security assessments related to third-party involvement, including cloud computing**,** which introduces new risks concerning data security [5, 7, 10]. However, the currently applied KAMI Index framework consists of five core domains**,** namely: (1) Information Security Policy; (2) Information Security Risk Management; (3) Information Security Framework; (4) Information Asset Management; (5) Technology and Information Security [7, 8, 10].

2.3. NIST

The National Institute of Standards and Technology (NIST) Framework is widely used for cybersecurity management across various sectors, featuring five core functions: Identify, Protect, Detect, Respond, and Recover [26, 43, 44]. In the United States, NIST is practically implemented in approximately 57.9% of industries [45]. These functions provide a holistic approach to addressing cybersecurity risks [26]. Each NIST framework serves a specific purpose while complementing the others. Thus, NIST SP 800-55 is particularly useful for organizations seeking to measure the effectiveness of their implemented security controls using performance metrics. It is highly suitable for security auditors, IT risk teams, and compliance management personnel aiming to ensure that security policies function effectively [46]. The commonalities among NIST CSF, NIST SP 800-53, and NIST SP 800-55 are their focus on cybersecurity, risk management, and their complementary roles in cybersecurity implementation [47, 48].

To effectively measure the ISMS, ISO/IEC 27001:2013 can be integrated with NIST Special Publications (NIST SP), particularly NIST SP 800-55. This framework is designed to establish and monitor security performance metrics, such as incident resolution time or the effectiveness of security training programs [4, 49]. Metrics play a crucial role in providing a pragmatic approach to monitoring security control performance and assessing overall security posture. This integration can be achieved through the mapping of ISO 27001 controls with NIST SP 800-55 [50]. NIST SP 800-55 v1 serves as a fundamental guide for designing information security measurement systems**,** helping organizations understand risks and enhance overall security. The first version (v.1) is a flexible framework for developing and selecting information security measures at the organizational, mission, or business, and system levels to assess the success of policies, procedures, and controls in place [42].

NIST SP 800-55 Rev. 1 consists of six (6) key metric categories, namely: Governance & Compliance, Risk Management, Access Control & Identity Management, Data Protection & Encryption, System Availability & Business Continuity, Threat Detection & Incident Response. Additionally, the framework defines 43 core metric elements [46]. The categories and metric elements of NIST SP 800-55 Rev.1 are presented in Table 1.

Table 1. Categories and metric elements NIST SP 800-55 Rev.1 [46]

Metric categories	Key metric elements	Description
Governance & Compliance metrics	Policy Compliance Rate, Regulatory Compliance Rate, Audit Finding Resolution Time	Metrics to measure compliance with security policies and regulations
Risk management metrics	Risk Management Effectiveness, Incident Response Time, Mean Time To Detect (MTTD)	Metrics for assessing the effectiveness of information security risk management
Access Control & Identity management metrics	Privileged Access Review Rate, User Account Revocation Time, Multi-Factor Authentication	Metrics for measuring user access and authentication security
Data Protection & Encryption metrics	Data Encryption Effectiveness, Backup Success Rate, Data Loss Prevention (DLP) Incident Rate	Metrics for assessing the effectiveness of encryption and data protection
System availability & Business continuity metrics	System Availability Rate, Disaster Recovery Readiness, Mean Time to Recover (MTTR)	Metrics for measuring system availability and recovery readiness
Threat detection & Incident response metrics	Time to Patch Critical Vulnerabilities, Security Log Monitoring Coverage, Percentage of Detected Attacks Blocked	Metrics to evaluate the effectiveness of threat detection and response

2.4. Integration of ISO 27001 with NIST

NIST and ISO are internationally recognized as best practices in information security systems and cybersecurity risk management. Integrating relevant controls from NIST frameworks and ISO standards can significantly enhance an organization's cybersecurity posture [51]. The managerial approach of ISO/IEC 27001 can be combined with specific controls from NIST, such as privacy management and system configuration, to establish a more comprehensive information security framework [15, 16, 26]. While ISO/IEC 27001 primarily focuses on information security standards and compliance, NIST emphasizes a flexible approach to cyber risk management[38]. ISO/IEC 27001 provides a structured methodology for information security management, incorporating specific controls such as encryption and incident management. However, its implementation is often complex and resource-intensive [38, 52]. Meanwhile, NIST SP 800-55 and ISO 27001:2013 exhibit a strong correlation in information security management, with NIST SP 800-55 focusing on security measurement metrics and ISO 27001 emphasizing security controls [52].

To evaluate multiple information security standards, such as ISO/IEC and NIST, while ensuring compliance across different frameworks and maintaining a core focus on the CIA, a mapping approach can be employed [28]. This integration can be achieved by aligning ISO 27001 controls with NIST SP 800-55 [50] and using security metrics to assess security maturity. The alignment between ISO 27001 and NIST SP 800-55 can be established through control mapping [50]. Moreover, ISO 27001 can be mapped to other security frameworks, including NIST SP 800-55, to support threat modeling analysis based on the STRIDE framework (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) [53].

3. Method

Based on the background and literature review discussed earlier, this study aims to map the alignment of security standards to assess information security risk maturity using NIST and ISO/IEC 27001:2013, with a primary focus on the CIA (Confidentiality, Integrity, Availability) triad during the transition to ISO/IEC 27001:2022. To achieve this objective, an alternative method is required that integrates maturity evaluation approaches, security risk management, and transition analysis of standards within private and government organizations in Indonesia, most of which utilize the KAMI Index standard. The methodology used in this research involves conducting security standard alignment mapping through an ontology-based mapping model for information security maturity assessment. Ontology serves as an instrument to address conceptual clarification issues and systematize terminology, providing a structured approach to formalizing security context knowledge necessary for proper security requirements implementation [45].

The domain mapping or key security areas are based on the primary focus of ISMS, namely CIA, as supported by previous studies [33, 36]. Mapping is essential to ensure that a single implemented standard can fulfill the requirements of another standard (cross-compliance). Furthermore, the collaboration between ISO 27001 as a managerial framework and NIST as a technical guideline is recommended by several researchers [28, 38, 51]. In this study, ISO/IEC 27001:2013 Annex A is integrated with NIST SP 800-55 to establish, monitor, and measure security performance metrics, aligning with prior research [4, 46, 49]. This integration is achieved by applying a security standard mapping model based on ontology-based mapping [54]. The research stages are illustrated in Fig. 1.

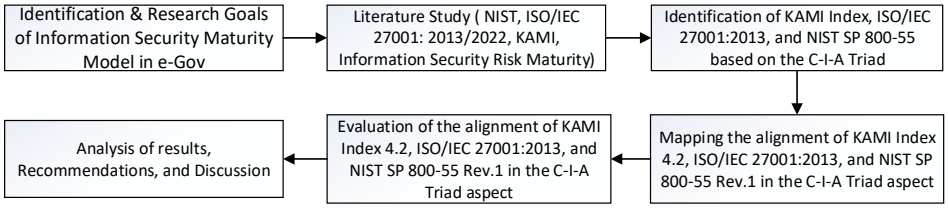

Fig. 1. Research stages

3.1. Identification of core security principles and security standards

The identification and description of the three core security areas (CIA Triad) are presented in Table 2. Each CIA security element in Table 2 possesses distinct characteristics and objectives**,** which serve as the foundation for mapping security standards to ensure compliance and alignment with best practices.

Next, the identification of all security standard elements is conducted by determining five (5) primary control domains from KAMI Index Version 4.2, fourteen (14) control areas from Annex A of ISO/IEC 27001:2023, and six (6) key metric categories from NIST SP 800-55 Rev.1. These elements are structured and presented in Table 3 to facilitate the alignment and cross-compliance mapping between the different security standards.

Table 2. Key Areas of information security [33, 35, 36, 43]

CIA Triad	Description	Security methods examples	Security threats examples
Confidentiality	Ensures information confidentiality by restricting access only to authorized individuals	Encryption, Access control, Multi-Factor Authentication (MFA)	Phishing attacks, Insider threats, Data leakage
Integrity	Guarantees data accuracy and consistency while preventing unauthorized modifications	Hashing, Digital signature, Redundancy checks	Data tampering, Man-in-the-Middle Attacks, Data corruption
Availability	Ensures that information and systems are available and accessible when needed	Data backup, Disaster recovery plan, High availability systems	DDoS attacks, Hardware failures, Ransomware

Table 3. Identification of Key Elements and Standard Security Controls

Primary security (CIA Triad)	KAMI Index Domain (Version 4.2)	Annex A ISO 27001:2013	NIST SP 800-55 (Rev. 1)
3 Main security [7, 9, 16]: • Confidentiality • Integrity • Availability	5 Main Domains of KAMI Index [7, 8, 10]: • Information Security Policy • Information Security Risk Management • Information Security Management Framework • Information Asset Management • Information technology and security (incident handling & recovery)	14 Control areas ISO 27001:2013 [8, 10]: • A.5 Information security policies • A.6 Organization of information security • A.7 Human resource security • A.8 Asset management • A.9 Access control • A.10 Cryptography • A.11 Physical and environmental security • A.12 Operation security • A.13 Communications security • A.14 System acquisition, development, and maintenance • A.15 Supplier relationships • A.16 Information security incident management • A.17 Information security aspects of business continuity management • A.18 Compliance	6 Key category metrics [42, 50]: • Governance & Compliance • Risk management • Access control & Identity management • Data protection & Encryption • System availability & Business continuity • Threat detection & Incident response.

3.2. Information security standard mapping model

The ontology-based mapping is performed by aligning each security control within the adopted security standards based on its semantic meaning. Ontology mapping refers to the alignment process that relies on the semantic interpretation of each control element within the security standards [45, 55]. Therefore, it is essential to identify and analyze the security standards currently used in Indonesia, namely: KAMI Index Version 4.2, ISO/IEC 27001:2013, and NIST SP 800-55 Revision 1. Mapping Process Steps:

1. Mapping the alignment of KAMI Index based on the Core Cybersecurity Principles (CIA Triad).

2. Mapping the alignment of KAMI Index with the 14 control domains of ISO 27001:2013 based on the CIA Triad.

3. Mapping the alignment of KAMI Index with the 14 control domains of ISO 27001:2013 and the 6 key metric categories of NIST SP 800-55 Rev.1 based on the CIA Triad.

4. Establishing an ontology-based mapping set to align KAMI Index version 4.2, the 14 primary control elements of ISO/IEC 27001:2013, and NIST SP 800-55 Rev.1 based on the CIA Triad.

5. Evaluating the alignment level among security standards using the Jaccard Similarity Index (JSI), calculated as:

(1) $$J(A, B)=|A \cup B||A \cap B|.$$

6. Validating the alignment model, compiling results, and providing recommendations.

4. Results and discussion

4.1. Mapping the alignment of information security

4.1.1. Mapping of KAMI Index with ISO based on CIA

The core cybersecurity principles, comprising the CIA Triad, serve as the fundamental security framework for standardized mapping. Therefore, each control domain of KAMI Index Version 4.2, which has been widely used as a cybersecurity standard in Indonesia**,** must first be aligned with the CIA. This step is essential before integrating it with other security standards. The mapping process ensures that each security standard aligns with others, verifying that control elements maintain compliance and interoperability across different standards. In this context, an ontology-based mapping approach is applied to align the CIA Triad with the control elements of the KAMI Index and ISO 27001.

The mapping of the primary domains of KAMI Index Version 4.2 with the 14 control areas from Annex A of ISO/IEC 27001:2013 is conducted after aligning the KAMI Index with the Core Security Principles (CIA Triad). The alignment of the CIA Triad with the KAMI index, including ISO 27001, is shown in Table 4. This approach is necessary because the development of KAMI Index domains is fundamentally based on ISO 27001. Applying an ontology-based mapping approach, the mapping process matches each domain element from both standards based on their semantic definitions. Based on Table 1, Table 2, and Table 3 above, the following control element alignment results can be further mapped, with the final results presented in Table 4.

From Table 4, it can be observed that the alignment map between the KAMI Index and ISO/IEC 27001:2013 illustrates that all five primary domains of the KAMI Index are interconnected with the 14 control areas in Annex A of ISO 27001. This correlation indicates that both standards can be used simultaneously, where the

KAMI Index assists organizations in evaluating information security maturity levels, while ISO 27001 provides a more technical implementation framework.

Table 4. Alignment Map of KAMMI and ISO 27001 Index based on CIA Triad

KAMI Index domain (Version 4.2)	Control domain annex A ISO/IEC 27001:2013	CIA Triad	Alignment description
1. Information security policy	**A.5** Information security policies	C, I, A	Ensure effective information security policies and governance for data protection
	A.6 Organization of information security	C, I, A	Establish responsibilities, information security structures, and leadership to support security implementation
2. Information security risk management	A.8 Asset management	C, I	Identify and manage information assets based on their value and associated risks
	A.12 Operation security	C, I, A	Assess operational risks, ensure implementation of effective operational policies to prevent data leakage or loss
3. Information security management framework	A.7 Human resource security	C, I	Managing human resource security, including information security training and awareness
	A.9 Access control	C, I	Control user access rights to ensure only authorized parties can access data
4. Information asset management	A.10 Cryptography	C, I	Securing data with encryption techniques to maintain the confidentiality and integrity of information
	A.11 Physical and environmental security	A	Protecting technology and information assets from physical threats such as natural disasters and theft
	A.14 System acquisition, development, and maintenance	C, I, A	Ensure that the development and maintenance of information systems is carried out with attention to security aspects
5. Information technology and security (incident handling & recovery)	A.13 Communications security	C, I	Ensuring the security of communications and data transmission within the organization to prevent information leakage
	A.15 Supplier relationships	C, I	Managing security risks in relationships with external partners or service providers
	A.16 Information security incident management	C, I, A	Provide an information security incident response system for impact mitigation and service recovery
	A.17 Information security aspects of business continuity management	A	Ensuring the continuity of organizational operations through preparedness for recovery from disasters or major incidents
	A.18 Compliance	C, I, A	Ensuring that the organization complies with applicable information security regulations and standards

Furthermore, the importance of the CIA Triad in mapping is evident, as it provides a clearer perspective on security principles: Confidentiality (C): Focuses on protecting data from unauthorized access, such as access control (A.9) and cryptography (A.10). Integrity (I): Ensures that data remains accurate and unmodified without authorization**,** exemplified by asset management (A.8) and communication security (A.13). Availability (A): Ensures that information and systems remain

accessible when needed, such as physical security (A.11) and business continuity management (A.17).

4.1.2. Benefits of security information implementation through mapping

a. Organizations can use the KAMI Index as a baseline evaluation before implementing ISO 27001.

b. Improve understanding of the relationship between national and international standards, enabling the implementation of best practices in information security management.

c. Bridge national regulatory compliance and global standards, fostering greater stakeholder trust.

Based on Table 4**,** a diagram can be created to provide a visual representation of the relationship between national and international security standards and how the CIA Triad is applied in information security management. The visualized diagram is presented in Fig. 2.

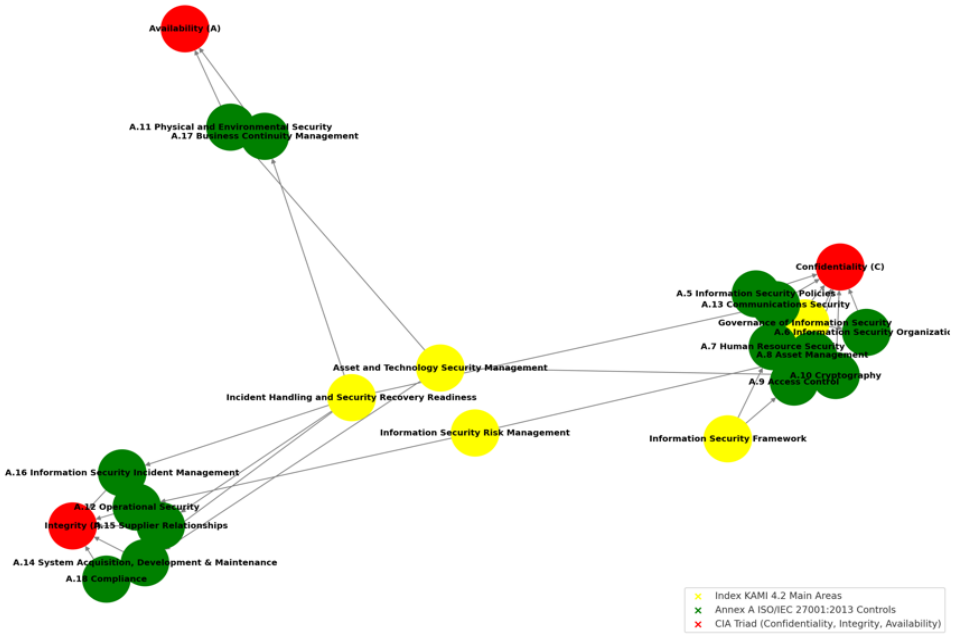

Fig. 2. Alignment relationship diagram between the CIA Triad and the main areas of the KAMI Index Version 4.2 and ISO/IEC 27001:2013

4.1.3. Mapping the KAMI Index, ISO 27001, CIA Triad, and NIST

The alignment mapping between the CIA Triad, the primary domains of the KAMI Index Version 4, and ISO/IEC 27001:2013 has been conducted as shown in Table 4 and Fig. 2. The next step involves mapping the five primary domains of the KAMI Index Version 4.2, the 14 control areas in Annex A of ISO/IEC 27001:2013, and the CIA Triad with the six key metric categories of NIST SP 800-55 Rev.1. This mapping aims to integrate multiple security standards and frameworks holistically to enhance the effectiveness of information security management within an organization.

The resulting alignment mapping is presented in Table 5.

Table 5. WE, ISO 27001, CIA, and NIST index alignment mapping

KAMI Index Domain (Version 4.2)	Control Domain Annex A ISO/IEC 27001:2013	CIA Triad	NIST SP 800-55 Rev.1 (6 Key Category Metrics)	Alignment description
1. Information security policy	A.5 Information security policies	C, I, A	Governance & Compliance	Set policies, roles, and responsibilities in information security, and ensure compliance with regulations and standards
	A.6 Organization of information security	C, I, A	Governance & Compliance	Establish security governance structures, roles, and responsibilities, and ensure compliance with information security policies
2. Information security risk management	A.8 Asset management	C, I	Risk Management	Identify, classify, and manage information assets according to the risks they face
	A.12 Operation security	C, I, A	Threat detection & Incident response	Ensure the security of information technology operations through system monitoring, threat detection, and response to security incidents
3. Information security management framework	A.7 Human resource security	C, I	Security training & Awareness	Increasing awareness and capacity of human resources in securing information through training and socialization
	A.9 Access control	C, I	Access control & Identity management	Manage access to information and systems so that only authorized parties have access through authentication and authorization mechanisms
4. Information asset management	A.10 Cryptography	C, I	Data protection & Encryption	Protecting data using encryption and other cryptographic methods to ensure the confidentiality and integrity of information
	A.11 Physical and environmental security	A	System availability & Business continuity	Securing physical infrastructure and work environment to maintain the operational sustainability of information systems
	A.14 System acquisition, development, and maintenance	C, I, A	System availability & Business continuity	Ensuring security aspects are implemented in the information systems development and maintenance life cycle
5. Information technology and security (incident handling & recovery)	A.13 Communications security	C, I	Data protection & Encryption	Securing organizational communications to prevent information leaks and data interception
	A.15 Supplier relationships	C, I	Governance & compliance	Manage security in relationships with external vendors and partners to mitigate information security supply chain risks
	A.16 Information security incident management	C, I, A	Threat detection & Incident response	Provide incident response and post-incident recovery mechanisms to minimize the impact of cyber attacks
	A.17 Information security aspects of business continuity management	A	System availability & Business continuity	Ensuring information systems remain operational and recover quickly after major disruptions or incidents
	A.18 Compliance	C, I, A	Governance & Compliance	Ensure compliance with information security standards and regulations to avoid legal and operational risks

The primary objectives include:

a. Improving compliance with both national and international standards, ensuring comprehensive coverage of all aspects of information security.

b. Enhancing threat detection capabilities and incident response effectiveness.
c. Increasing efficiency in information security risk management.
d. Assisting organizations in prioritizing security enhancements.

Based on Table 5, it is evident that each domain within the KAMI Index has a clear correspondence with ISO 27001 and NIST SP 800-55 Rev.1. This indicates that these standards can be implemented simultaneously to enhance information security management. ISO 27001:2013 provides a structured framework for implementing information security controls. NIST SP 800-55 Rev.1 offers evaluation metrics to assess the effectiveness of security controls. The KAMI Index can be utilized to measure an organization's readiness in Indonesia for adopting international security standards. The Role of the CIA Triad in the Mapping Process:

a. Confidentiality (C). Protecting information access, including Security policies (A.5), Access control (A.9), and Cryptography (A.10).

b. Integrity (I). Ensuring data accuracy and reliability, including Asset management (A.8), Communication security (A.13), and Incident management (A.16).

c. Availability (A). Ensuring that information and systems remain accessible when needed, including Business continuity (A.17) and Physical security (A.11).

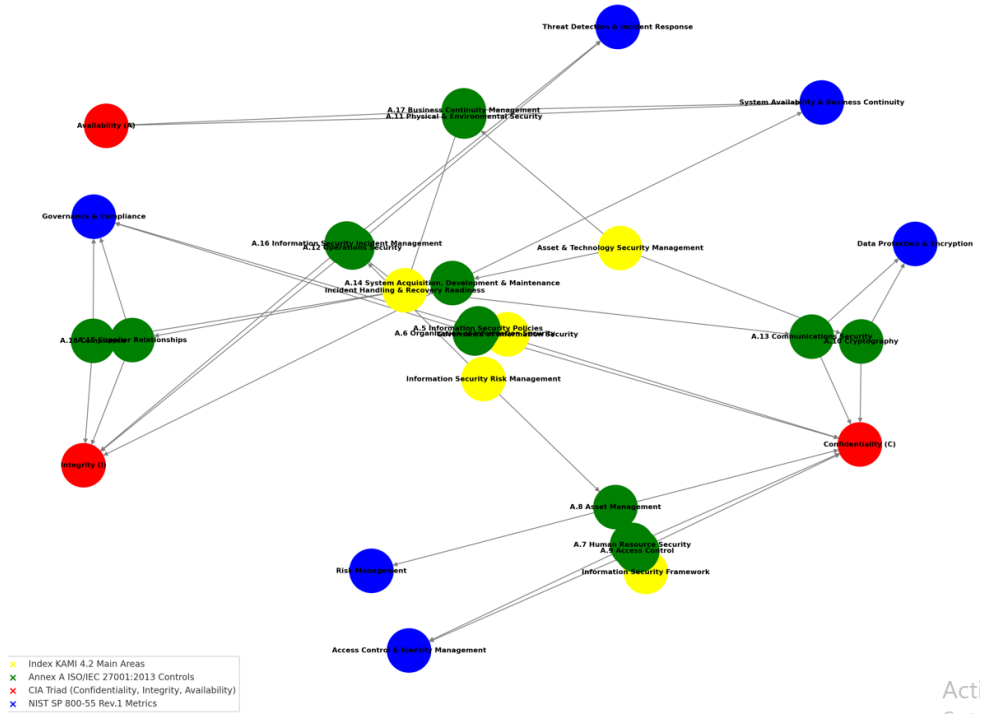

Fig. 3. Alignment relationship diagram between the CIA Triad and the main areas of the KAMI Index Version 4.2, ISO/IEC 27001:2013, and NISP SP 800-55 Rev.1

The ontology alignment diagram in Fig. 3 illustrates the relationship and interconnection between the five primary domains of the KAMI Index 4.2, the 14 security controls in Annex A of ISO/IEC 27001:2013, the CIA Triad, and the six key

metric categories of NIST SP 800-55 Rev.1. This mapping holds strategic significance for organizations in effectively managing information security through a holistic, measurable, and standardized approach that aligns with both global and national standards**.** The mapping process ensures that the national standard (KAMI Index) can be adopted and strengthened by global standards (ISO 27001 & NIST SP 800-55 Rev.1). This approach enables organizations to adopt national standards without disregarding international best practices, thereby enhancing their readiness to address global information security challenges. Additionally, organizations can ensure that implemented information security policies are truly effective by utilizing appropriate performance metrics**,** prioritizing security reinforcements based on risks associated with the CIA Triad. Furthermore, leverage a risk-based approach with a more objective and data-driven evaluation system. Align security policies, risk strategies, and operational security within a unified and coherent system.

4.2. Evaluation of security standard alignment mapping

Based on the alignment mapping results between the five primary domains of KAMI Index Version 4.2, the 14 security controls in Annex A of ISO/IEC 27001:2013, and the six primary domains of NIST SP 800-55 Rev.1, which are aligned with the core security principles of the CIA Triad, an evaluation of security standard alignment mapping can be conducted. This alignment mapping is illustrated through ontology-based integration, as shown in Table 4 and Fig. 2, as well as Table 5 and Fig. 3. These mappings demonstrate that the national security standard (KAMI Index) can be effectively integrated with ISO/IEC 27001 and NIST SP 800-55. Additionally, the CIA Triad serves as the foundational framework for assessing the effectiveness of security controls across different standards. The diagrams highlight the conceptual similarities between national and international security frameworks, indicating a high degree of alignment and compatibility. To assess the degree of alignment among security standards, the Jaccard Similarity Index (JSI) is employed, calculated using Equation (1) as follows: $J(A, B)=|A \cup B||A \cap B|$. Calculation steps:

Step 1. Defining the Concept Sets for Each Security Standard: KAMI Index 4.2 → 5 primary concepts, ISO/IEC 27001:2013 → 14 security controls, CIA Triad → 3 core security principles, NIST SP 800-55 Rev.1 → 6 key metric elements

Step 2. Computing the Common Elements (Intersection $|A \cap B|$):

a. The number of overlapping concepts based on the mapping diagram (i.e., concepts appearing in more than one standard).

b. Examples extracted from the diagram:

– Governance & Compliance (KAMI Index) ↔ A.5 (ISO) ↔ Governance & Compliance (NIST)

– Risk management (KAMI Index) ↔ A.8 (ISO) ↔ Risk management (NIST)

– Threat detection & Incident response (NIST) ↔ A.16 (ISO) ↔ Incident handling & Recovery readiness (KAMI Index)

From this data, we estimate that $|A \cap B| = 10$ overlapping concepts.

Step 3. Computing the Union ($|A \cup B|$):

a. The total unique elements across all standards (without duplication).

b. Given that: KAMI Index has 5 primary domains, ISO 27001 has 14 security controls, CIA Triad has 3 security principles, NIST SP 800-55 has 6 key metrics, and 10 overlapping elements. The union ($|A \cup B|$) is calculated as

$$|A \cup B| = 5 + 14 + 3 + 6 - 10 = 18.$$

Step 4. Calculating the Jaccard Similarity Index (JSI):

a. Total unique values across all standards (without duplicates) is

$$5 + 14 + 3 + 6 = 28$$

b. Total duplicated values (appearing in more than one standard): 10

c. Thus, the JSI calculation is

$$J(A, B) = |A \cap B| / |A \cup B| = 10/18 = 0.56 \ (56\%)$$

This result indicates that there is a 56% alignment between the security standards. According to the JSI threshold**,** a 56% similarity score is considered a relatively high degree of alignment, signifying that these security frameworks can be effectively integrated to enhance information security management.

4.3. Analysis of results, recommendations, and discussion

4.3.1. Analysis of results

The alignment score between KAMI Index, ISO/IEC 27001, and NIST SP 800-55 Rev.1 was calculated as 0.56 (56%), positioning it within the moderate range ($0.4 \leq JSI \leq 0.7$). This indicates that the alignment among security standards has not yet reached a strong or high level ($JSI > 0.7$). This result suggests that while a significant portion of security concepts can be mapped across these standards**,** structural and terminological differences still require further harmonization**.** The standards exhibit considerable overlap in governance, risk management, access control, and business continuity, yet some aspects remain unique to each framework. However, the CIA Triad is well integrated with ISO 27001 security controls and NIST SP 800-55 evaluation metrics, demonstrating that international standards inherently incorporate fundamental information security principles. Some security standards share overlapping concepts, such as Governance & Compliance in NIST SP 800-55 and ISO 27001, which correspond to Information Security Governance in the KAMI Index.

Several security domains still require harmonization due to differences in evaluation structures, terminology, and the lack of evaluation metrics in the KAMI Index. Differences in evaluation structures include the KAMI Index, which adopts a maturity-based security assessment approach, while ISO 27001 is based on the Implementation of Security Controls (ISMS), and NIST SP 800-55 follows a measurement-based security evaluation model. These differences make it challenging to directly compare certain security controls across these standards. Terminological differences in the KAMI Index cannot be directly mapped to ISO 27001 or NIST SP 800-55 without further interpretation. For example, “Asset and Technology Management” in the KAMI Index needs to be decomposed into two separate components, namely “Security Asset Management” (A.8 in ISO 27001) and “Infrastructure Management” (A.14 in ISO 27001). The lack of evaluation metrics in the KAMI Index, unlike NIST SP 800-55, which adopts a metric-driven approach,

makes it necessary to adapt this standard to include data-driven evaluation elements to ensure a more objective and measurable security assessment.

4.3.2. Recommendations

To enhance the alignment between KAMI Index, ISO/IEC 27001:2013, and NIST SP 800-55 Rev.1, several recommendations are proposed:

1. Harmonizing terminology and concepts to ensure consistency across standards.
2. Developing an integrated maturity evaluation framework to bridge differences in assessment methodologies.
3. Incorporating these standards into national security policies to establish a unified regulatory framework.
4. These findings can be considered when implementing the KAMI index with the latest version (revised).

Additionally, further research is essential to explore more recent versions of these security standards, such as KAMI Index version 5.0, ISO/IEC 27001:2022, and NIST SP 800-55 Rev.2, to align with advancements in cybersecurity and evolving technological landscapes.

4.3.3. Discussion

Based on the findings of this study, several challenges and future research directions can be discussed:

1. Implications of Findings. The 56% alignment score indicates that these standards are compatible but not yet fully harmonized. Differences in evaluation structures and terminology present challenges in achieving full alignment. The CIA Triad has proven to be an effective foundation for security standard alignment, but a more comprehensive metric-based evaluation approach is needed.
2. Research Limitations. The mapping process was conducted based on core security concepts without considering the detailed implementation of security controls within organizations. The 56% JSI score is still indicative and requires further validation through case studies and in-depth analysis. More expert input from information security specialists is required to refine the ontology-based mapping model.
3. Future Steps. Ontology Model Validation with Real-World Cases: To assess its practical applicability, the ontology mapping framework should be tested in organizations that have implemented ISO 27001, KAMI Index, or NIST SP 800-55. Next, an Ontology-Based evaluation tool should be developed, and maturity evaluation metrics should be tested.

5. Conclusion

Based on the ontology mapping evaluation, the alignment level between KAMI Index, ISO/IEC 27001, and NIST SP 800-55, measured using the CIA Triad, was found to be 56%, indicating partial alignment but still requiring further harmonization. Harmonization is necessary in terms of terminology, evaluation methodologies, and integration into national regulations to improve standard

alignment. Additionally, a comprehensive information security maturity evaluation framework is needed to unify approaches from these three standards**.** Further validation through case studies and empirical testing is essential to refine the ontology model and ensure its practical applicability in real-world security management.

References

1. Al-Suqri, M. N., M. Gillani. A Comparative Analysis of Information and Artificial Intelligence Toward National Security. – IEEE Access, Vol. **10**, 2022, pp. 64420-64434.
2. Lee, G., S. Kim, I. Lee, S. Brown, Y. A. Carbajal. Adapting Cybersecurity Maturity Models for Resource-Constrained Settings: A Case Study of Peru. – The Electronic Journal of Information Systems in Developing Countries, Vol. **91**, 2025, No 1, e12350.
3. Pigola, A., P. R. da Costa. Cybersecurity Management: An Empirical Analysis of the Dynamic Capabilities Framework for Enhancing Cybersecurity Intelligence. – Information & Computer Security, 2025.
4. Aminudin, A., A. Supriyanto. Kematangan Risiko Keamanan Informasi Layanan TI Menggunakan Pendekatan NIST dan Standart ISO 27001: 2013 (Studi Kasus: Bapenda Provinsi Jawa Tengah). – AITI, Vol. **21**, 2024, No 2, pp. 210-229.
5. Savitri, R., F. Firmansyah, D. Dworo, M. S. Hasibuan. Information Security Measurement Using INDEX KAMI at Metro City. – Journal of Applied Data Sciences, Vol. **5**, 2024, No 1, pp. 33-45.
6. Wardhani, W. K., B. Soewito, M. Zarlis. Information Security Evaluation Using Case Study Information Security Index on Licensing Portal Applications. – Journal of Information Systems and Informatics, Vol. **5**, 2023, No 4, pp. 1204-1220.
7. Nugroho, S., T. Rochmadi. Analysis of Information Security Readiness Using the Index KAMI. – Decode: Jurnal Pendidikan Teknologi Informasi, Vol. **4**, 2024, No 3, pp. 881-886.
8. Sugiarto, P., Y. Suryanto. Evaluation of the Readiness Level of Information System Security at the BAKAMLA Using the KAMI Index Based on ISO 27001: 2013. – Int. J. Mech. Eng., Vol. **7**, 2022, No 2, pp. 3607-3614.
9. Sofyan, H., W. Kaswidjanti, L. S. Ilmiyah. Information Security Index (ISI) 4.2 for Information Security Evaluation (Case Study: Sleman Regency Communication and Informatics Office). – In: Proc. of 1st International Conference on Advanced Informatics and Intelligent Information Systems (ICAI3S'23), 2023, Atlantis Press, 2024, pp. 188-200.
10. Waruwu, M., A. Indrati. IDN Media Information Security Management System Maturity Measurement Analysis Using ISO 27001: 2013 and KAMI Index Version 4.0. – International Research Journal of Advanced Engineering and Science, Vol. **6**, 2021, No 3, pp. 36-40.
11. Suorsa, M., P. Helo. Information Security Failures Identified and Measured-ISO/IEC 27001:2013 Controls Ranked Based on GDPR Penalty Case Analysis. – Information Security Journal, Vol. **33**, 2024, No 3, pp. 285-306.
12. Juma, A. H., A. A. Arman, F. Hidayat. Cybersecurity Assessment Framework: A Systematic Review. – In: Proc. of 10th International Conference on ICT for Smart Society, ICISS 2023, Institute of Electrical and Electronics Engineers Inc., 2023.
13. Apriany, A., A. Wibowo. Analysis of the Implementation of ISO 27001: 2022 and KAMI Index in Enhancing the Information Security Management System in Consulting Firms. – IJCCS (Indonesian Journal of Computing and Cybernetics Systems), Vol. **18**, 2024, No 4, pp. 417-428.
14. Putro, P. A. W., D. I. Sensuse, W. S. S. Wibowo. Framework for Critical Information Infrastructure Protection in Smart Government: A Case Study in Indonesia. – Information and Computer Security, Vol. **32**, 2024, No 1, pp. 112-129.
15. Kurii, Y., I. Opirsky y. Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001: 2013. – NIST Spec. Publ., Vol. **800**, 2022, No 3, pp. 21-32.

16. Sulistyowati, D., F. Handayani, Y. Suryanto. Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002, and PCI DSS. – JOIV: International Journal on Informatics Visualization, Vol. **4**, 2020, No 4, pp. 225-230.
17. Schrödter, A., B. E. Weißenberger. The Institutionalization of Digital Compliance. – Management Decision, 2024.
18. Raditya, M., P. Dewanto, T. Oktavia, D. Sundaram. Comparative Study of Information Security Evaluation Models for the Indonesian Government. – Journal of Theoretical and Applied Information Technology, Vol. **28**, 2022, pp. 895-914.
19. Supriyanto, A., K. Mustofa. E-Gov Readiness Assessment to Determine the e-Government Maturity Phase. – In: Proc. of 2nd International Conference on Science in Information Technology (ICSITech'16), 2016, Information Science for Green Society and Environment, 2017, pp. 270-275.
20. Gupta, K., V. Mishra, A. Makkar. A Global Cybersecurity Standardization Framework for Healthcare Informatics. – IEEE Journal of Biomedical and Health Informatics, 2024, pp. 1-8.
21. Vakhula, O., Y. Kurii, I. Opirskyy, V. Susukailo. Security as Code Concept for Fulfilling ISO/IEC 27001: 2022 Requirements. – In: CPITS, 2024, pp. 59-72.
22. Djebbar, F., K. Nordstrom. A Comparative Analysis of Industrial Cybersecurity Standards. – IEEE Access, Vol. **11**, 2023, pp. 85315-85332.
23. Singh, A. K., B. D. K. Patro. Security of Low Computing Power Devices: A Survey of Requirements, Challenges & Possible Solutions. – Cybernetics and Information Technologies, Vol. **19**, 2019, No 1, pp. 133-164.
24. Wicaksono, A. C., S. Prabowo, D. Oktaria. Risk and Security Measurement Based on ISO 27001 Using FMEA Methodology Case Study of: National Government Agency. – In: Proc. of 1st International Conference on Software Engineering and Information Technology, ICoSEIT 2022, Institute of Electrical and Electronics Engineers, Inc., 2022, pp. 6-11.
25. Dhirani, L. L., E. Armstrong, T. Newe. Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. – Sensors, Vol. **21**, 2021, No 11, pp. 1-30.
26. Gujar, S. S., D. Thiyagarajan, S. Sudesh Sakpal, A. K. Pandey. Advanced Cybersecurity Frameworks for Protecting Sensitive Information in Academic Libraries: Innovations and Best Practices. Library of Progress – Library Science. – Information Technology & Computer, Vol. **4**, 2024, No 3, pp. 198-209.
27. Djebbar, F., K. Nordstrom. A Comparative Analysis of Industrial Cybersecurity Standards. – IEEE Access, Vol. **11**, 2023, pp. 85315-85332.
28. Boyes, H., M. D. Higgins. An Overview of Information and Cyber Security Standards. – Journal of ICT Standardization, Vol. **12**, 2024, No 1, pp. 95-134.
29. Diamantopoulou, V., A. Tsohou, M. Karyda. From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR Compliance Controls. – Information and Computer Security, Vol. **28**, 2020, No 4, pp. 645-662.
30. Malatji, M. Management of Enterprise Cyber Security: A Review of ISO/IEC 27001:2022. – In: Proc. of International Conference on Cyber Management and Engineering (CyMaEn'23), Institute of Electrical and Electronics Engineers, Inc., 2023, pp. 117-122.
31. Valavanis, S. Understanding Cybersecurity Maturity in Practice. – Journal of Information Systems, Vol. **38**, 2024, No 3, pp. 1-5.
32. Miloslavskaya, N., S. Tolstaya. Information Security Management Maturity Models. – In: Procedia Computer Science. Vol. **213**. Elsevier B. V., 2022, pp. 49-57.
33. Rajak, C., J. Bharti, A. Mateen, N. Mehndiratta, J. Chauhan, R. Marndi. A Roadmap to ISMS ISO 27001 Implementation Process. – In: Proc. of 3rd International Conference on Range Technology (ICORT'23), Institute of Electrical and Electronics Engineers, Inc., 2023.
34. Supriyanto, A., D. A. DIartono, B. Hartono, H. Februariyanti. Inclusive Security Models to Building e-Government Trust (ICICOS'19) – In: Proc. of 3rd International Conference on Informatics and Computational Sciences: Accelerating Informatics and Computational Research for Smarter Society in the Era of Industry 4.0, Proceedings, 2019.

35. Supriyanto, A., J. E. Istiyanto, K. Mustofa. Multi-Layer Framework for Security and Privacy-Based Risk Evaluation on e-Government. – Journal of Theoretical and Applied Information Technology, Vol. **97**, 2019, No 5, pp. 1423-1433.
36. Azinheira, B., M. Antunes, M. Maximiano, R. Gomes. A Methodology for Mapping Cybersecurity Standards into Governance Guidelines for SME in Portugal. – In: Procedia Computer Science. Vol. **219**. Elsevier B. V., 2023, pp. 121-128.
37. Guo, H., M. Wei, P. Huang, E. G. Chekole. Enhance Enterprise Security through Implementing ISO/IEC 27001 Standard. – In: Proc. of IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI'21), 2021, Institute of Electrical and Electronics Engineers, Inc., 2021.
38. Salihu, A., R. Dervishi. Evaluating the Impact of Risk Management Frameworks on IT Audits: A Comparative Analysis of COSO, COBIT, ISO/IEC 27001, and NIST CSF. – In: Proc. of International Conference on Electrical, Communication and Computer Engineering (ICECCE'24), IEEE, 2024, pp. 1-8.
39. Culot, G., G. Nassimbeni, M. Podrecca, M. Sartor. The ISO/IEC 27001 Information Security Management Standard: Literature Review and Theory-Based Research Agenda. – TQM Journal, Emerald Group Holdings, Ltd., Vol. **33**, 2021, No 7, pp. 76-105.
40. Otoom, A. A., I. Atoum, H. Al-Harahsheh, M. Aljawarneh, M. N. Al Refai, M. Baklizi. A Collaborative Cybersecurity Framework for Higher Education. – Information & Computer Security, September 2024.
41. Savitri, R., F. Firmansyah, D. Dworo, M. S. Hasibuan. Information Security Measurement Using INDEX KAMI at Metro City. – Journal of Applied Data Sciences, Vol. **5**, 2024, No 1, pp. 33-45.
42. Kitsios, F., E. Chatzidimitriou, M. Kamariotou. The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. – Sustainability (Switzerland), Vol. **15**, 2023, No 7, pp. 2-17.
43. Supriyanto, A., D. A. Diartono, B. Hartono, H. Februariyanti. Inclusive Security Models for Building e-Government Trust. – In: Proc. of 3rd International Conference on Informatics and Computational Sciences (ICICoS'19), October 2019, pp. 1-6.
44. Hochstetter-Diez, J., M. Diéguez-Rebolledo, J. Fenner-López, C. Cachero. AIM Triad: A Prioritization Strategy for Public Institutions to Improve Information Security Maturity. – Applied Sciences (Switzerland), Vol. **13**, 2023, No 14, pp. 2-29.
45. Peldszus, S., J. Bürger, T. Kehrer, J. Jürjens. Ontology-Driven Evolution of Software Security. – Data and Knowledge Engineering, Vol. **134**, 2021, No May, pp. 1-25.
46. Schroeder, K., V. Y. Pillitteri, K. Schroeder, V. Y. Pillitteri. NIST Special Publication 800 Measurement Guide for Information Security. – Measurement Guide for Information Security Volume 1 – Identifying and Selecting Measures, Vol. **1**, 2024.
47. Amiruddin, A., H. G. Afiansyah, H. A. Nugroho. Cyber-Risk Management Planning Using NIST CSF V1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8. – In: Proc. of 3rd International Conference on Informatics, Multimedia, Cyber, and Information System, (ICIMCIS'21), Institute of Electrical and Electronics Engineers, Inc., 2021, pp. 19-24.
48. Hamdani, S. W. A., H. Abbas, A. R. Janjua, W. B. Shahid, M. F. Amjad, J. Malik, A. W. Khan. Cybersecurity Standards in the Context of Operating Systems: Practical Aspects, Analysis, and Comparisons. – ACM Computing Surveys (CSUR), Vol. **54**, 2021, No 3, pp. 1-36.
49. Tintin, R., M. Hidalgo. Could an ISMS Model (ISO/IEC 27001:2013 Standard) Implementation Protect Public Data?. – In: Proc. of 9th International Conference on eDemocracy and e-Government, ICEDEG 2023, Institute of Electrical and Electronics Engineers, Inc., 2023.
50. Kielland, C. Information Security Performance Evaluation: Building a Security Metrics Library and Visualization Dashboard (Master's Thesis). 2023.
51. Ngalim, B. Integrating NIST and ISO Cybersecurity Audit and Risk Assessment Frameworks into Cameroonian Law. – Journal of Cybersecurity Education Research and Practice, Vol. **2024**, 2023, No 1, pp. 1-9.
52. Alshar'e, M. Cyber Security Framework Selection: Comparison of Nist and Iso27001. – Applied Computing Journal, Vol. **3**, 2023, No 1, pp. 245-255.

53. S e t i a w a n, H., N. A. H a n a, R. R. H a n a p u t r a. Mapping ISO 27001: 2013 and COBIT 2019 Framework to STRIDE Threat Modelling Using Qualitative Descriptive Research. – Journal of Computer Engineering, Electronics and Information Technology, Vol. **3**, 2023, No 2, pp. 101-110.
54. M u s s m a n n, A., M. B r u n n e r, R. B r e u. Mapping the State of Security Standards Mappings. – In: Proc. of 15th International Conference on Business Information Systems 2020 "Developments, Opportunities and Challenges of Digitization". – In: Wirtschaftsinformatik (Zentrale Tracks). 2020, pp. 1309-1324.
55. A h m a d, F., M. F a i s a l. Assessing Similarity between Software Requirements: A Semantic Approach. – International Journal of Information Engineering and Electronic Business, Vol. **15**, 2023, No 2, pp. 38-53.

Received: 12.02.2025, Revised Version: 03.04.2025, Accepted: 16.04.2025