Jurnal Informatika: Jurnal pengembangan IT

Vol. 10, No. 1, 2025
ISSN : 2477-5126, DOI:10.30591/jpit.v10i1.8211

Analysis of Information Security Management System Implementation at BSN

Kiki Puspo Arianty [1]
[1] *Universitas Asa Indonesia, Jl. Raya Kalimalang No. 2A, Jakarta, 13430, Indonesia*

Info Artikel

Riwayat Artikel:

Received 2025-01-03
Revised 2025-01-06
Accepted 2025-01-07

Corresponding Author:

Kiki Puspo Arianty

Email: kiki@asaindo.ac.id

Abstract – *SNI ISO/IEC 27001:2013, adopted by the National Standardization Agency of Indonesia (BSN), is a national standard derived from the international ISO/IEC 27001 published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This study evaluates the effectiveness of BSN's Information Security Management System (ISMS) implementation, focusing on compliance with international standards, risk management strategies, and organizational commitment to safeguarding information. Employing qualitative descriptive methods, data were collected through interviews, document analysis, and observations. The findings highlight the critical roles of leadership commitment, comprehensive risk assessments, and regular system evaluations in achieving ISMS objectives. Despite significant achievements, including obtaining Integrated Management System certification in 2023, challenges persist in optimizing resources and adapting to emerging security threats. Recommendations include enhancing staff capabilities, investing in advanced technologies, and transitioning to the updated SNI ISO/IEC 27001:2022 standard. This study reinforces the importance of ISMS in protecting sensitive information, fostering trust, and aligning with global best practices.*

Keywords: *Information Security Management System, SNI ISO/IEC 27001:2013, National Standardization Agency of Indonesia, BSN, Risk Management, Information Security*

Abstrak – *SNI ISO/IEC 27001:2013, yang diadopsi oleh Badan Standardisasi Nasional (BSN), merupakan standar nasional yang berasal dari standar internasional ISO/IEC 27001 yang diterbitkan oleh International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC). Penelitian ini mengevaluasi efektivitas implementasi Sistem Manajemen Keamanan Informasi (SMKI) di BSN, dengan fokus pada kepatuhan terhadap SNI yang merupakan adopsi dari standar internasional, strategi manajemen risiko, dan komitmen organisasi dalam menjaga keamanan informasi. Metode deskriptif kualitatif digunakan dengan pengumpulan data melalui wawancara, analisis dokumen, dan observasi. Hasil penelitian menunjukkan pentingnya komitmen kepemimpinan, penilaian risiko yang komprehensif, dan evaluasi sistem secara berkala dalam mencapai tujuan SMKI. Meskipun BSN telah meraih sertifikasi Sistem Manajemen Terintegrasi pada 2023, tantangan masih ada, seperti optimalisasi sumber daya dan adaptasi terhadap ancaman keamanan yang terus berkembang. Rekomendasi mencakup peningkatan kompetensi staf, investasi pada teknologi canggih, dan transisi ke standar SNI ISO/IEC 27001:2022 yang telah diperbarui. Studi ini menegaskan pentingnya peran SMKI dalam melindungi informasi sensitif, meningkatkan kepercayaan, dan selaras dengan praktik terbaik global.*

Kata Kunci*: Sistem Manajemen Keamanan Informasi, SNI ISO/IEC 27001:2013, Badan Standardisasi Nasional, Manajemen Risiko, Keamanan Informasi*

I. Introduction

On June 20, 2024, Indonesia's National Data Center (Pusat Data Nasional, PDN) faced a ransomware attack known as "Brain Cipher," a variant of LockBit 3.0 ransomware. This cyberattack disrupted various public services, including immigration services, causing significant delays in the processing of visas, passports, and residence permits nationwide. At least 210 institutions were impacted, and numerous sectors experienced severe disruptions due to this incident.

Hackers reportedly demanded a ransom of USD 8 million (approximately IDR 131 billion) to decrypt the affected data. Although the Indonesian government did not confirm whether the ransom was paid, the attack underscored vulnerabilities in the country's digital security systems. It also highlighted the critical need for robust data protection measures to secure the digital infrastructure of government systems.

This incident served as a stark reminder of the importance of implementing a solid information security system, particularly in government agencies handling sensitive data. As the digital era continues to evolve, threats like ransomware can cause substantial losses and disrupt vital public services. Strengthening information security management systems across governmental institutions is, therefore, essential to safeguard data continuity and security.

In today's millennial society, the growth of IT extends beyond the industrial sector and has also been adopted by the government sector, which has implemented IT management.[1]

The case demonstrated that threats to information security cannot be ignored and require proactive measures to prevent similar incidents in the future. It also emphasized the need for strict standards in managing information security to ensure the proper protection of managed data.

Information security refers to efforts to protect information assets from various potential threats. The primary goal of information security is to ensure business continuity, reduce risks, and maximize return on investment.[2] As organizations manage, store, and share increasing amounts of data, the risk of damage, loss, or unauthorized access to this data also grows.

Information security plays a critical role in safeguarding an organization's information assets. Based on the classification by Whitman and Mattord, information security can be divided into several types:[3]

a. Physical Security: Focuses on protecting the physical safety of personnel, assets, and facilities from threats such as fire, unauthorized access, and natural disasters.
b. Personal Security: Protects individuals within the organization, often overlapping with physical security.
c. Operational Security: Ensures the smooth operation of organizational processes without interference.
d. Communications Security: Protects communication media, technologies, and the content of communications.
e. Network Security: Focuses on securing network devices and ensuring the safe transmission of data.

Information security is built on three core elements, commonly referred to as the CIA Triad. These three elements are interdependent and must all be achieved to ensure optimal information security:[4]

a. Confidentiality: Ensures that information is accessible only to authorized parties.
b. Integrity: Maintains the accuracy and completeness of information, preventing alterations whether intentional or accidental.
c. Availability: Ensures that information is accessible when needed.

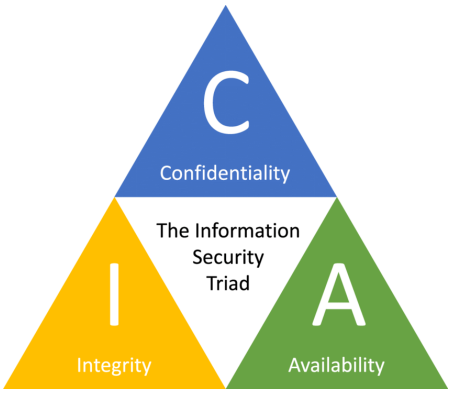

Figure 1. The Confidentiality, Integrity, Availability (CIA) Triad[5]

As a non-ministerial government agency responsible for standardization and conformity assessment (standardisasi dan penilaian kesesuaian/SPK), the National Standardization Agency of Indonesia (Badan Standardisasi Nasional/BSN) plays a pivotal role in establishing the Indonesian National Standards (Standar Nasional Indonesia/SNI) as the only national standard applicable throughout Indonesia. Under Law (Undang-undang) No. 20 of 2014 on Standardization and Conformity Assessment, BSN is tasked with improving the quality and competitiveness of Indonesian products while protecting society from risks that could threaten health, safety, security, and the environment. Therefore, information security is crucial for BSN, not only for internal data management but also for maintaining public trust and ensuring the smooth execution of standardization processes that significantly impact various industrial sectors in Indonesia.[6]

The importance of information security at BSN is further underscored by its role as a national standard-setting body. The data and information managed by BSN relate to various standards and conformity assessments, covering critical aspects of industries, health, the environment, and more. If these data are not managed properly, risks such as data breaches, manipulation, or other cyber threats could negatively impact the national standardization process and erode public and industrial trust in BSN's role.

An Information Security Management System (ISMS) is a framework used to manage and control information security. It involves a structured process that is documented and recognized across the organization. The strategies and policies within it are designed to protect the confidentiality, availability, and integrity of information assets, while maintaining a risk level that the organization is willing to accept.[7]

One international standard relevant to maintaining information security is ISO/IEC 27001. This standard provides a systematic framework for managing an information security management system (ISMS). ISO/IEC 27001:2013 includes policies, procedures, and controls designed to identify, manage, and mitigate risks to information security.

The ISO/IEC 27001 is a management framework that helps identify, assess, and develop solutions for potential risks. It provides guidance to organizations in creating an information security plan tailored to their specific needs. When an organization chooses to implement an information security strategy, it must first establish its own approach to effectively manage information security risks and threats, while ensuring the sustainability of a strategy that aligns with ISO/IEC 27001 standards.[8]

SNI ISO/IEC 27001:2013 is an information security standard adopted by BSN from the international ISO/IEC 27001 standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This standard is designed to help organizations manage information security systematically and effectively. Its implementation minimizes the risk of data breaches while enhancing trust from business partners and the public.

This standard outlines the criteria for setting up, executing, maintaining, and continuously enhancing an ISMS in the context of the organization. It also covers the requirements for evaluating and addressing information security risks based on the organization's specific needs. The requirements outlined in this standard are general and are intended to be applicable to all organizations, regardless of their type, size, or sector. Any omission of the requirements specified in Clauses 4 to 10 is not permissible when an organization claims compliance with this standard.[9]

Implementing this standard enables organizations to ensure the safety, integrity, and availability of their data. For a government agency like BSN, implementing this standard is essential to protect all data and information related to SNI from both internal and external threats.

BSN demonstrated its commitment to information security by obtaining the SNI ISO/IEC 27001:2013 certification in 2019 from PT Sucofindo, a Management System Certification Body accredited by The National Accreditation Body of Indonesia (Komite Akreditasi Nasional/KAN). This certification serves as evidence that BSN has implemented an information security management system that complies with national and international standards, including risk management, staff training, and the implementation of policies and procedures that support data security.

However, as technology evolves and cyber threats grow in complexity, periodic evaluations are necessary to ensure the continued effectiveness and relevance of the implemented system. Such evaluations are also vital for identifying potential weaknesses in the system and providing recommendations for improvement to enhance information security at BSN.

Furthermore, evaluating the implementation of SNI ISO/IEC 27001:2013 at BSN aims to ensure compliance with the standard. Through this evaluation, BSN can assess the effectiveness of its policies and procedures in addressing cyber threats. The evaluation can also help identify areas needing improvement and provide data for developing better information security strategies in the future. This is particularly important given BSN's role in establishing standards followed by various industrial sectors in Indonesia, ensuring that public trust in this institution is maintained through robust and reliable information security practices.

Additionally, SNI ISO/IEC 27001:2013 serves as a reference for managing information security systems nationally and internationally. This standard allows organizations to adopt a consistent approach to addressing information security issues. By implementing this standard, BSN ensures that its data management aligns with global best practices, thereby enhancing its reputation and trust in the services it provides.

Moreover, adopting this standard supports BSN's objective of increasing the competitiveness of Indonesian products in the global market by ensuring that information related to conformity assessment processes remains secure and protected.

Therefore, a comprehensive evaluation of SNI ISO/IEC 27001:2013 implementation at BSN is necessary to ensure that the existing information security management system is effective, adaptable to changes, and aligned with technological advancements and the latest regulations. This evaluation not only ensures compliance with the standard but also acts as a proactive measure to mitigate future risks.

Through a thorough evaluation, BSN can identify areas for improvement, optimize risk management, and enhance the overall effectiveness of its information security system. In doing so, BSN can continue to fulfill its role as a credible and trusted standardization body in Indonesia.

The research question focuses on evaluating the implementation of the information security management system based on SNI ISO/IEC 27001:2013 at BSN. Therefore, the problem statement is detailed into the following research questions:

1. How is the implementation of the information security management system based on ISO 27001:2013 at BSN?
2. What are the obstacles encountered in implementing the standard?
3. How effective is the implementation of the ISMS in protecting information at BSN?

Based on the problem statement, the research objectives are to:

1. Evaluate the implementation of ISO 27001:2013 at BSN.
2. Identify the factors that hinder and drive the implementation of the ISMS at BSN.

3. Provide recommendations for improving the information security management system at BSN.

II. Metodology

A. Type of Research

This study employs a qualitative descriptive method with a case study approach conducted at the National Standardization Agency (BSN). This method allows the researcher to gain an in-depth understanding of the implementation of the Information Security Management System (ISMS) at BSN and its underlying context. The qualitative descriptive research method involves studying an object, condition, group of people, or other phenomena in their natural or real setting (without an experimental background) to provide an accurate, systematic, and detailed description.[10]

B. Location and Duration of the Research

The research was conducted at BSN over a designated period of three months, starting in October 2024 and concluding in December 2024. The choice of location is highly relevant due to BSN's critical role in standardization and the implementation of information security policies in Indonesia.

C. Data Sources

The research subjects are individuals and processes within BSN.

a. Primary Data: Primary data is defined as a data source that directly provides data to the data collector. [11] Collected through interviews with management, IT staff, and ISMS users at BSN. The purpose is to explore their experiences and perspectives regarding the implemented information security policies and the challenges encountered.
b. Secondary Data: Secondary data is data obtained from graphic documents (tables, records, meeting minutes, SMS, and others), photographs, films, video recordings, and other objects that can enrich primary data. [12] Secondary data sources include information security policy documents, internal audit reports, and literature related to SNI ISO/IEC 27001:2013. This secondary data provides important additional context for analyzing ISMS implementation at BSN.

D. Data Collection Techniques

1) Semi-Structured Interviews: This technique is employed to gather in-depth information about the experiences and views of informants regarding ISMS implementation. The semi-structured format allows the researcher to adjust questions based on the responses provided. A semi-structured interview is a type of interview in which informants can provide answers freely without strict limitations, yet they must still adhere to the predetermined theme.[13]

   The interviews were conducted as follows:

TABLE 1
INTERVIEW SCHEDULE

No.	Date/Day	Location	Name	Position
1.	Tuesday, November 26, 2024	Zoom Meeting	Akbar Aryanto	Senior Computer Officer/Head of the Infrastructure and Information Security Team at BSN
2.	Tuesday, November 26, 2024	Zoom Meeting	Rizky Mulya Akbar	Junior Computer Officer/Head of the Information Systems and Data Governance Team at BSN

2) Documentation: Documentation is a form of evidence about something, including records, photos, video recordings, or anything produced by a researcher. These documents represent moments that have already passed and are likely to generate the information, facts, and data required in the research.[14] This involved reviewing documents related to information security policies, procedures, and records at BSN. This process was essential for understanding the legal and procedural framework underlying the implementation of ISMS.
3) Observation: Observation is a direct examination conducted by the researcher on the research subject or a specific environment, which can be either active or passive observation.[15] The researcher conducted direct observations of the processes and procedures applied in ISMS implementation at BSN. This provided practical insights into the execution of information security policies.

E. Data Analysis Methods

1) Descriptive Analysis: This technique is used to describe the implementation of the ISMS at BSN. Data obtained from interviews and observations will be analyzed to identify patterns and themes emerging in the implementation of the ISMS.

2) Application of the SNI ISO/IEC 27001:2013 Framework: This framework will serve as an evaluation tool to assess the compliance and effectiveness of the information security management system at BSN. The objective is to evaluate the extent to which BSN meets the established standards. The SNI ISO/IEC 27001:2013 standard consists of key components, including clauses that outline the mandatory requirements organizations must fulfill when implementing an ISMS based on the established framework.[9]

TABLE 2
CLAUSES IN SNI ISO/IEC 27001:2013

No.	Clause
1	Scope
2	Normative References
3	Term and Definitions
4	Context of The Organization
4.1	Understanding the Organization and Its Context
4.2	Understanding the Needs and Expectations of Interested Parties
4.3	Determining the Scope of the Information Security Management System
4.4	Information Security Management System
5	Leadership
5.1	Leadership and commitment
5.2	Policy
5.3	Organizational roles, responsibilities and authorities
6	Planning
6.1	Actions to address risks and opportunities
6.2	Information security objectives and planning to achieve them
7	Support
7.1	Resources
7.2	Competence
7.3	Awareness
7.4	Communication
7.5	Documented information
8	Operation
8.1	Operational planning and control
8.2	Information security risk assessment
8.3	Information security risk treatment
9	Performance Evaluation
9.1	Monitoring, measurement, analysis and evaluation
9.2	Internal audit
9.3	Management review
10	Improvement
10.1	Nonconformity and corrective action
10.2	Continual improvement

3) SWOT Analysis (Strengths, Weaknesses, Opportunities, and Threats): Organizations looking for effective solutions and strong strategies for their operations can use SWOT, tailoring it to their specific needs and circumstances. The standardized application of SWOT analysis follows a template that offers essential guidelines for evaluating an organization's future prospects. This analysis is organized around identifying factors that could either support or obstruct the achievement of the organization's goals. In SWOT, key questions revolve around identifying where our strengths and weaknesses lie, as well as the types of threats and opportunities we may encounter.[16] SWOT analysis will be used to identify strengths and weaknesses in the ISMS implementation at BSN, as well as opportunities and threats faced. The resulting recommendations are expected to provide input for further improvement and development.

III. Results and Discussion

A. History of ISMS Implementation at BSN

BSN began implementing the Information Security Management System (ISMS) in 2018. Initially, this implementation was focused on the scope of the Data Center and Information Systems. BSN's commitment to protecting critical information from security threats was realized with the achievement of the SNI ISO/IEC 27001:2013 certification in 2019 from PT Sucofindo.

Aligned with BSN's vision to enhance bureaucratic efficiency and effectiveness, a policy to integrate management systems was introduced in 2021. This integration covered three major management systems standards: SNI ISO 9001:2015 for Quality Management Systems, SNI ISO/IEC 27001:2013 for Information Security Management Systems, and SNI ISO 37001:2016 for Anti-Bribery Management Systems. With this policy, the scope of ISMS implementation was expanded to encompass all work units within BSN.

The integration journey reached its peak in 2023. After undergoing various stages of audits and evaluations, BSN successfully obtained the Integrated Management System certificate from PT Sucofindo on May 7, 2023. This certification is valid until 2026 and serves as tangible evidence that BSN has met national and international standards in three critical management domains.

B. Organizational Context (Clause 4)

BSN faces various external and internal issues that influence the objectives and success of the ISMS.

1) External Issues
   a. Policies, Regulations, and National Development Plans
      1. Government policies encouraging the implementation of the Electronic-Based Government System (SPBE).
      2. The COVID-19 pandemic driving the development of emergency response systems.
      3. Policies to accelerate the prevention of corruption relevant to implementing information security policies at BSN.
      4. Government Regulation No. 33 of 2023 on Energy Conservation, which affects resource management efficiency.
      5. Presidential Regulation No. 111 of 2022 on Sustainable Development, governing sustainability management in government institutions.
   b. Stakeholder Awareness and Trust
      1. Demands for BSN services through efficient and secure electronic applications.
      2. Lack of consumer awareness about SNI-certified products, impacting the overall effectiveness of standard implementation.
   c. The Role of Standardization in Global Economic Development
      1. Information security challenges in cross-border electronic transactions.
      2. BSN's collaboration with international organizations, such as ISO, IEC, and others, to strengthen information security standards.
      3. Incomplete harmonization of international standards, limiting SNI product acceptance in global markets.

2) Internal Issues
   a. Availability, Quality, and Capacity of Resources
      1. Limited IT infrastructure to securely support BSN's main tasks and functions.
      2. Suboptimal integration of electronic applications for efficient information management.
      3. Optimization of the roles of BSN's five Technical Service Offices (KLT) to support ISMS implementation regionally.
   b. Management Systems, Values, and Organizational Culture
      1. Management of confidential information not fully aligned with SPBE standards.
      2. Need for quality training services to enhance human resource competencies in information security.
      3. Green Office *policy, including energy savings and operational cost efficiency.*
   c. Organizational Performance
      1. BSN's financial management status, receiving a WTP (Unqualified Opinion) from the Audit Board of Indonesia (BPK).
      2. Government recognition for financial management and performance achievements.
      3. International acknowledgment for accreditation services (LPK) and National Metrology System Unit (SNSU) management.

4. BSN's performance measured by services free from corruption, collusion, and nepotism (KKN).

The identified external and internal factors significantly influence the successful implementation of ISMS at BSN. Understanding these issues is a key element in supporting a comprehensive and standard-compliant information security strategy.

In the context of Clause 4.1 "Understanding the Organization and Its Context", analyzing external issues, such as government policies on SPBE implementation and regulatory impacts, allows BSN to identify risks and opportunities that may affect information security. For instance, implementing energy conservation and sustainability policies creates opportunities to enhance resource efficiency while addressing challenges in digital data management.

Clause 4.2 "Understanding the Needs and Expectations of Interested Parties" emphasizes the importance of mapping stakeholder needs, including the demand for efficient and secure electronic applications. By meeting these expectations, BSN can enhance public trust and uphold its reputation as a responsible institution in national standardization.

The application of Clause 4.4 "Information Security Management System" requires a holistic approach to information security management. This includes strategic management of internal resources, such as optimizing the roles of Technical Service Offices (KLT) and integrating electronic applications to support operational efficiency.

C. Leadership (Clause 5)

The commitment of top management serves as the cornerstone for implementing ISMS. The Head of BSN consistently supports system development through policies integrated with BSN's Strategic Plan (Renstra), in alignment with Clause 5.1 "Leadership and Commitment." These policies reflect the organization's strategic direction.

The dissemination of information security policies is conducted through media such as flyers distributed via WhatsApp and awareness videos shown during Monday morning assemblies, supporting Clause 5.2 "Information Security Policy."

Additionally, the active role of management in regularly emphasizing the importance of information security demonstrates adherence to Clause 5.3 "Organizational Roles, Responsibilities, and Authorities."

As outlined in Annex A.6 "Information Security Organization," the successful implementation of ISMS at BSN relies on a clear organizational structure and well-defined responsibilities. This ensures that all personnel understand their roles in safeguarding information, minimizing risks from internal sources.

D. Planning (Clause 6)

BSN identifies and evaluates information security risks through its Risk Management Task Force. This approach supports Clause 6.1 "Actions to Address Risks and Opportunities." The primary reference is BSN Regulation (Peraturan BSN) No. 4 of 2021 on Risk Management.

E. Support (Clause 7)

Top management actively promotes the importance of information security to all employees. Communication is conducted through management review outcomes distributed by the integrated management system secretariat and through directives during Monday morning assemblies. These practices align with Clause 7.4 "Communication," which governs communication within the ISMS framework.

Policies are disseminated through internal media to foster awareness and compliance among all employees. Additionally, physical threat protection remains a critical focus. Annex A.11 "Physical and Environmental Security" requires BSN to implement adequate security measures for infrastructure, such as data center facilities, ensuring protection against damage or unauthorized access to information assets.

F. Operation (Clause 8)

BSN ensures ISMS operations by managing risks in accordance with Clause 8.1 "Operational Planning and Control." Risk identification and evaluation are carried out by the Risk Management Task Force (Satgas).

This team conducts quarterly monitoring and evaluation (M&E) to ensure ISMS implementation in all organizational units complies with standards, supporting Clause 8.2 "Information Security Risk Assessment," which emphasizes ongoing risk assessment.

To address information security incidents, BSN has established a Computer Security Incident Response Team (CSIRT) that coordinates with the National Cyber and Crypto Agency (BSSN). Members are selected based on relevant competencies, ensuring compliance with Annex A.16 "Information Security Incident Management," which governs incident handling.

In managing information security risks, BSN employs measures outlined in Clause 8.3 "Information Security Risk Treatment."Relationships with external parties, such as partners and vendors, involve managing security risks in external interactions, including the implementation of appropriate operational measures. Annex A.15 "Supplier

Relationships" highlights the importance of maintaining information security in all external engagements, whether through contractual agreements or related risk management.

G. Performance Evaluation (Clause 9)

Information security policies are reviewed at least annually through internal and external audits, in alignment with Clause 9.3 "Management Review." This process ensures policy relevance and effectiveness.

Internal audits are conducted by BSN's Risk Management Task Force, while external audits are performed by PT Sucofindo.

H. Improvement (Clause 10)

Nonconformities are identified through risk evaluations, with corrective actions implemented to mitigate risks, in accordance with Clause 10.1 "Nonconformity and Corrective Action." Information security policies are continuously updated to ensure compliance, supporting Clause 10.2 "Continual Improvement."

TABLE 3
IMPLEMENTATION OF THE INFORMATION SECURITY MANAGEMENT SYSTEM AT BSN BASED ON SNI ISO/IEC 27001:2013 CLAUSES

No.	Clause	Information
1	Organizational Context (4)	**Clause 4.1 "Understanding the Organization and Its Context"**: BSN analyzes external and internal issues such as government policies on SPBE, COVID-19 emergency systems, anti-corruption, energy conservation (PP No. 33/2023), and sustainability (Perpres No. 111/2022). Internal issues include limited IT infrastructure, suboptimal electronic application integration, and the need for better KLT optimization. **Clause 4.2 "Understanding the Needs and Expectations of Interested Parties"**: Addresses stakeholder demands for efficient and secure electronic applications, and increasing awareness of SNI-certified products. **Clause 4.4 "Information Security Management System"**: Ensures holistic management, including resource optimization, technical service office roles, and digital integration to enhance operational efficiency.
2	Leadership (5)	**Clause 5.1 "Leadership and Commitment"**: Top management ensures ISMS integration with BSN's Strategic Plan (Renstra). **Clause 5.2 "Information Security Policy"**: Policies are disseminated through flyers, WhatsApp, and videos during assemblies. **Clause 5.3 "Organizational Roles, Responsibilities, and Authorities"**: Organizational structure ensures clear roles in safeguarding information.
3	Planning (6)	**Clause 6.1 "Actions to Address Risks and Opportunities"**: Risks are identified and evaluated by the Risk Management Task Force, guided by BSN Regulation No. 4 of 2021.
4	Support (7)	**Clause 7.4 "Communication"**: Security policies are communicated through management system reviews and Monday assemblies. **Annex A.11 "Physical and Environmental Security"**: Measures implemented to protect infrastructure such as data centers from physical and environmental threats.
5	Operation (8)	**Clause 8.1 "Operational Planning and Control"**: ISMS operations managed by Risk Management Task Force. **Clause 8.2 "Information Security Risk Assessment"**: Risk evaluations are carried out through monitoring and evaluation (M&E). **Annex A.16 "Information Security Incident Management"**: CSIRT coordinates incident handling with BSSN. **Annex A.15 "Supplier Relationships"**: Security risks managed in external partnerships and operational engagements.
6	Performance Evaluation (9)	**Clause 9.3 "Management Review"**: Policies are reviewed annually through internal audits by the Risk Management Task Force and external audits by PT Sucofindo, a Management System Certification Body accredited by The National Accreditation Body of Indonesia (KAN), to ensure relevance and effectiveness.
7	Improvement (10)	**Clause 10.1 "Nonconformity and Corrective Action"**: Corrective actions implemented to address risks. **Clause 10.2 "Continual Improvement"**: Policies are continuously updated to comply with evolving standards and improve ISMS effectiveness.

I. Implications of the Study

1) Strengthening ISMS Implementation Strategies

This study highlights BSN's journey in implementing ISMS, starting with an initial focus on the Data Center and Information Systems, and later integrating it with other management systems. The success of this phased and integrated approach emphasizes the importance of such a strategy in ISMS implementation, which can serve as a guide for other organizations in managing information security more effectively. Moreover, the Integrated Management System certification obtained by BSN from PT Sucofindo, a Management System

Certification Body accredited by the National Accreditation Body of Indonesia (KAN), stands as concrete evidence that ISMS implementation not only enhances information security but also helps organizations meet with national and international standards.

2) Impact of External and Internal Factors on ISMS

External factors such as government policies, the COVID-19 pandemic, and the demands of cross-border electronic transactions present both challenges and opportunities for managing information security. Conversely, internal factors such as limited IT infrastructure and the need for improved human resource competencies highlight that the success of ISMS requires optimal resource management. This analysis provides insights into how organizations can navigate external and internal issues to ensure the sustainability of ISMS.

3) The Importance of Leadership and Organizational Culture

The study emphasizes that top management's commitment is a cornerstone of ISMS success. Consistent support from BSN leadership, such as integrating information security policies with the organization's strategic plans, illustrates how strong leadership can foster awareness and compliance across all organizational levels. It also underscores the importance of cultivating an organizational culture where information security is a core value, ensuring that every individual understands their role in safeguarding data integrity.

J. Contribution to the Development of ISMS Practices

By employing the SNI ISO/IEC 27001:2013 standards, this study not only provides a comprehensive understanding of ISMS implementation but also offers an evidence-based approach to continuous improvement. Processes such as audits, risk evaluations, and the establishment of an incident response team serve as best practices that other organizations can adopt. Additionally, the integration with other standards, such as quality management and anti-bribery systems, demonstrates how a holistic approach can strengthen the overall management framework of an organization.

IV. Conclusion

The implementation of the Information Security Management System (ISMS) based on ISO 27001:2013 at the National Standardization Agency (BSN) has been carried out effectively and has successfully achieved the various objectives that were set. Since its inception in 2018, BSN has implemented an integrated information security policy within a broader management system. BSN also achieved ISO/IEC 27001:2013 certification in 2019 and Integrated Management System certification in 2023, demonstrating its serious commitment to protecting critical information. However, the implementation of this system has faced several challenges, both internally and externally. Based on the evaluation results, the following are the conclusions regarding the implementation of ISMS at BSN.

1. Implementation of the Information Security Management System at BSN
   The implementation of ISMS at BSN has been in accordance with ISO/IEC 27001:2013 standards, reflected in the integration of the information security policy with the quality management system (SNI ISO 9001:2015) and anti-bribery system (SNI ISO 37001:2016). The top management of BSN has demonstrated a strong commitment to supporting the implementation of ISMS, manifested in structured and integrated policies. BSN has also formed a competent team and conducts regular training to ensure that every employee understands the importance of information security. Additionally, ongoing evaluation and auditing policies serve as an effective oversight mechanism.
2. Challenges in Implementing ISO 27001:2013
   BSN faces several obstacles in implementing ISMS, particularly related to limited resources and IT infrastructure. Some of the existing IT systems have not fully supported the optimal information security needs, which can slow down the implementation of existing policies. Additionally, organizational cultural resistance presents a unique challenge, considering the cultural shift required to consistently support the implementation of information security policies. To address this, BSN has implemented a more intensive awareness program and an inclusive approach involving all stakeholders to ensure the success of the implementation.
3. Effectiveness of ISMS Implementation in Protecting Information
   The implementation of ISMS at BSN has proven effective in protecting the information it manages. One key aspect of this success is the ongoing risk management implementation. BSN regularly identifies and evaluates information security risks through the Risk Management Task Force (Satgas), which operates according to BSN Regulation Number 4 of 2021 on BSN Risk Management. This team performs quarterly monitoring and evaluation (monev) to ensure that every unit within BSN complies with the established information security standards and policies. This approach is in line with Clause 6.1 of ISO/IEC 27001:2013, which outlines actions

to address risks and opportunities. Furthermore, BSN has also formed a Computer Security Incident Response Team (CSIRT), tasked with handling information security incidents. The CSIRT collaborates with the National Cyber and Encryption Agency (BSSN) and is selected based on relevant competencies to ensure prompt and accurate incident handling. The existence of this team supports compliance with Clause 16 of ISO/IEC 27001:2013, which governs information security incident management.

Overall, the implementation of ISMS at BSN aligns with the SNI standards adopted from international standards and has provided significant protection for the managed information. Despite challenges in resource management and organizational culture shifts, BSN has effectively managed risks through routine and systematic risk evaluations. The ongoing risk management approach, along with the establishment of the CSIRT, ensures that each security threat can be identified and handled effectively. The sustainability and effectiveness of this ISMS implementation are proof that BSN is capable of maintaining information security with a high level of protection.

Based on the evaluation results that have been presented, there are several strategic steps that BSN can take to further strengthen the implementation of the Information Security Management System (ISMS). The following recommendations aim to ensure the sustainability and effectiveness of the integrated management system that has been implemented, while also supporting the achievement of the organization's overall objectives.

1. Enhancing Human Resource Competency: BSN needs to continue enhancing employee competencies through more intensive training related to information security, risk management, and anti-bribery. This training should cover both technical and non-technical aspects, so that every employee can better understand and effectively implement the information security policies.
2. Technology Investment: Given the growing cyber threats, BSN needs to make larger investments in information security technologies. This includes the procurement of software and hardware that can help detect, prevent, and address increasingly complex threats, such as ransomware attacks or data breaches.
3. Strengthening the Information Security Culture: BSN needs to reinforce the information security culture at all levels of the organization. Awareness programs should be more intensive, such as by holding routine and incentive-based training to encourage each individual to be more attentive and responsive to information security issues. Involving all employees in the security policy can increase the effectiveness of the existing system.
4. Collaboration with External Parties: To strengthen the implementation of ISMS, BSN can expand collaborations with other relevant institutions or agencies, both at the national and international levels, in order to gain new insights and perspectives in addressing information security challenges. This collaboration will also ensure that the implementation of ISMS remains relevant to the latest regulatory and standard developments.
5. Ongoing Monitoring: Monitoring and evaluation should be reinforced on a regular basis. BSN needs to increase the frequency of evaluations and audits to identify potential gaps in the system and ensure that the management system remains aligned with the evolving threats and organizational needs. This approach will also help maintain the reliability of the system that has been implemented.
6. Preparation for Transition to SNI ISO/IEC 27001:2022: BSN should begin preparing for the transition to SNI ISO/IEC 27001:2022. This process includes analyzing changes in the requirements of the new standard, updating relevant documents, and providing training and transition audit simulations to ensure the implementation goes smoothly without disrupting the ongoing operations.

References

[1] A. Fathurohman and R. W. Witjaksono, "Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City)," *Bull. Comput. Sci. Electr. Eng.*, vol. 1, no. 1, pp. 1–11, 2020, doi: 10.25008/bcsee.v1i1.2.

[2] A. H. Harahap, C. Difa Andani, A. Christie, D. Nurhaliza, and A. Fauzi, "Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder," *J. Manaj. dan Pemasar. Digit.*, vol. 1, no. 2, pp. 73–83, 2023.

[3] S. Paramita, "Analisis Manajemen TIK Terhadap Keamanan Informasi Dan Manajemen Risiko Perpustakaan," *J. Teknol. dan Manaj. Sist. Ind.*, vol. 2, no. 1, pp. 54–61, 2023, doi: 10.56071/jtmsi.v2i1.469.

[4] I. Gaidarski and P. Kutinchev, "Some Aspects of Information Security and Cybersecurity Problem Area," *Probl. Eng. Cybern. Robot.*, vol. 79, pp. 55–66, 2023, doi: 10.7546/pecr.79.23.03.

[5] J. Nikander, O. Manninen, and M. Laajalahti, "Requirements for cybersecurity in agricultural communication networks," *Comput. Electron. Agric.*, vol. 179, no. September, p. 105776, 2020, doi: 10.1016/j.compag.2020.105776.

[6] K. Puspo and Y. Shintya, "INFORMASI AKSES SNI DENGAN METODE E-GOVQUAL DAN IPA Service Quality Analysis of SNI Access Information System with E-Govqual Method and IPA," vol. 6, no. 2, 2023.

[7] O. A. Fonseca-Herrera, A. E. Rojas, and H. Florez, "A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard," *IAENG Int. J. Comput. Sci.*, vol. 48, no. 2, pp. 1–10, 2021.

[8] F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, "The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector," *Sustain.*, vol. 15, no. 7, 2023, doi: 10.3390/su15075828.

[9] ISO 27001, "Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan Information technology – Security techniques – Information security management systems – Requirements," p. 54, 2013.

[10] Ageng Saepudin Kanda and Ratna Intan Sari, "Analisis Penerapan Sistem Informasi Manajemen Email IMS Di PT. IBU," *J. Publ. Sist. Inf. dan Manaj. Bisnis*, vol. 3, no. 2, pp. 109–119, 2024, doi: 10.55606/jupsim.v3i2.2772.

[11] R. O. Waruwu *et al.*, "Digital Di Dinas Komunikasi Dan Informatika Kabupaten Nias Utara Operation of the E-Archive Application

System in Maximizing the Operation Management of Digital-Based Incoming and Outgoing Mail Services At the Communication and Information Office of North," *J. Emba*, vol. 12, no. 1, pp. 1044–1051, 2024.

[12] N. Hidaya and I. Jatnika, "Perancangan Sistem Manajemen Keamanan Informasi Data Center Standard SNI ISO IEC 27001 2013," *JUSIM (Jurnal Sist. Inf. Musiwaras)*, vol. 7, no. 1, pp. 24–36, 2022, [Online]. Available: https://www.jurnal.univbinainsan.ac.id/index.php/jusim/article/view/1420%0Ahttps://www.jurnal.univbinainsan.ac.id/index.php/jusim/article/download/1420/797

[13] K. P. Gerupuk and K. L. Tengah, "3 1,2,3," vol. 13, no. 1, pp. 11–18, 2024.

[14] B. K. Tias, "Sistem Informasi Perluasan Pangsa Pasar Menggunakan Pendekatan Metode Bauran Pemasaran," *J. Teknol. dan Sist. Inf.*, vol. 4, no. 1Tias, Betty Kusumaning. 2021. "Sistem Informasi Perluasan Pangsa Pasar Menggunakan Pendekatan Metode Bauran Pemasaran." Jurnal Teknologi dan Sistem Informasi 4(1): 1–8., pp. 1–8, 2021.

[15] M. Tampubolon, *Metode Penelitian Metode Penelitian*, vol. 3, no. 17. 2023. [Online]. Available: http://repository.unpas.ac.id/30547/5/BAB III.pdf

[16] M. K. Akman, "SWOT Analysis and Security Management," *Eur. J. Manag. Mark. Stud.*, vol. 4, no. 2, pp. 78–89, 2019, doi: 10.5281/zenodo.3471920.