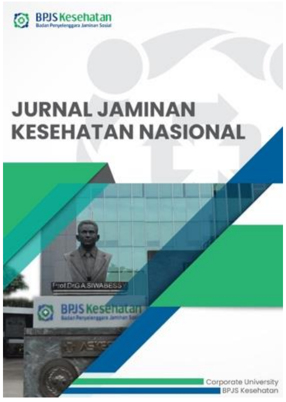
Jurnal Jaminan Kesehatan Nasional
Volume 5 Number 1, (June, 2025). Page 62 - 74
DOI: 10.53756/jjkn.v5i1.247
ISSN : 2798-6705 (online) | 2798-7183 (print)

Research Paper



Information Security Management System (ISMS) at BPJS Kesehatan Tondano: Implementation of ISO 27001:2022 Standard

Randa Matthew Iroth[1]

[1]BPJS Kesehatan, Tondano, Indonesia

Abstract: Information security is crucial for organizations managing sensitive data in the digital era. This is especially true for institutions like the Social Security Administrative Body for Health (BPJS Kesehatan), which organizes social health security for the Indonesian people and handles various important information, including participant, medical, and financial data. However, as threats to information security increase, organizations need to implement an effective information security management system. This research examines the implementation of the Information Security Management System (ISMS) based on the ISO 27001:2022 standard at the Tondano BPJS Kesehatan Branch Office. The methodology of the research is descriptive qualitative. The research results indicate that implementing the ISMS has improved overall data security. This is achieved through regular data backups and storing servers in locked rooms. In addition, implementing the ISO 27001:2022 standard reduces information security risks by providing clear guidance on data security management, including antivirus updates, access restrictions, and password management. The main challenges in implementing the ISMS are limited IT infrastructure resources and employee resistance to changes in IT security procedures. Despite these challenges, implementing the ISO 27001:2022 standard at the Tondano BPJS Kesehatan Branch Office has improved information security and strengthened the trust of customers and business partners.

Keywords: Information Technology; ISO 27001:2022; Social Health Security

Introduction

In the context of rapid technological development, the challenges faced by organizations in maintaining information security are increasingly complex. In the era of rapid digitalization, information security is one of the most crucial aspects for organizations that manage sensitive data, including BPJS Kesehatan. As an institution responsible for implementing social health security for the people of Indonesia, BPJS Kesehatan manages various important information, ranging from membership data to medical and financial information. Information security in Indonesia is still lagging compared to other Southeast Asian countries. Information leaks occur at the individual

Corresponding author name can be contacted at: 240253.randa@bpjs-kesehatan.go.id

level and in government institutions, where hackers still often manage to access important data (Suryono, 2023). Data security can indirectly ensure business continuity and reduce risk; the more corporate data is collected, organized, and distributed, the greater the risk of damage, loss, or data exposure to unwanted external parties (Lambi, 2023). Therefore, information security is one of the most crucial aspects for organizations. Technology development will also be followed by increased security vulnerabilities that can be a serious threat. Information security must also be the main focus to minimize all organizational risks (Pujian & Bisma, 2024).

With increasing threats to information security, organizations need to implement an effective information security management system (Paramita et al., 2022). Information security is very important in today's digital era because information has great value and plays a role in various aspects of life. In 2024, companies must prioritize mitigating digital, technological, and cyber risks, including information security (Fatih, 2024).

ISMS is a systematic framework for protecting information from potential threats that could cause damage. It includes security technologies, tools, policies, procedures, and processes designed to manage information risks comprehensively (Yustanti et al., 2018). Information Security Management Systems offer an organized way to manage and protect sensitive information (Soesanto et al., 2018). Information security management aims to protect data confidentiality, integrity, and accessibility (Fauzi, 2018).

Information security threats, such as cyberattacks, human error, and system failures, can lead to financial losses and damage the reputation and trust of customers and business partners. By managing information security well, companies can minimize the possibility of negative impacts and maximize positive results from their data and information (Lenawati et al., 2017). Therefore, information security is crucial to ensure that company information is accurate and continues to meet the company's evolving needs. With increasing threats to data security, privacy violations, and increasingly stringent regulations, BPJS Kesehatan must ensure its information management system can protect data effectively.

ISO 27001 is an international standard for information security management systems that can help meet information security needs of government agencies and other organizations (Suryono, 2023). By implementing the ISO 27001:2022 standard, organizations can systematically identify, manage, and mitigate information security risks. These standards also help build a strong security culture, increase awareness of the importance of security, and ensure compliance with applicable laws, regulations, and contracts (Sinaga, 2023).

Implementing an Information Security Management System (ISMS) and the ISO 27001:2013 standard positively affects information security and the overall performance of PT Surveyor Indonesia Surabaya Branch. These impacts include enhancing overall data security, mitigating risks, fostering trust among customers and business partners, and implementing rigorous information security practices (Prawiranata, 2024). The ISO 27001 standard is considered very suitable for application in various types of organizations, including higher education environments, as it focuses on information system security management and can be adapted to the specific needs of each organization (Winanti & Dzullhan, 2018; Pamungkas & Saputra, 2020; Drljača & Latinović, 2016).

This research aims to investigate the implementation of the Information Security Management System (ISMS) at the Tondano BPJS Kesehatan Branch Office. It will examine the implementation of ISMS based on the ISO 27001:2022 standard in the company's business operations.

Method

This research employs a qualitative approach with a descriptive analysis method to describe and examine the implementation of the Information Security Management System (ISMS) based on the ISO 27001:2022 standard at the BPJS Kesehatan Tondano Branch Office. This approach aims to provide a systematic and objective description of the actual condition of information security controls' application, based on information from relevant informants.

Informants in this study were selected using a purposive sampling technique, namely the deliberate selection of individuals who are considered to have an understanding and direct involvement in the implementation of ISMS. The interviews were conducted with five informants selected based on their roles in implementing the Information Security Management System (ISMS) at the Tondano BPJS Kesehatan Branch Office.

The interviews were conducted with five informants selected based on their roles in implementing the Information Security Management System (ISMS) at the Tondano BPJS Kesehatan Branch Office, as shown in Table 1. The selected participants represent a cross-section of roles critical to the ISMS implementation at the branch office. Data was collected through semi-structured interviews, guided by guidelines based on the four ISO 27001:2022 control groups: organizational control, people control, physical control, and technology control. Instrument validation was conducted through a preliminary study with three information security experts to ensure the clarity and suitability of the questions.

Table 1. Participants Profile

Participant	Post	Role
1	ISMS Officer	ISMS Coordinator
2	Head of Technology Information	ISMS Coordinator
3	Technology Information Officer	ISMS Implementer
4	Human Resources Officer	ISMS Implementer
5	Membership Officer	ISMS Implementer

Source: data processed (2025)

Interviews were conducted in person for 30 to 45 minutes, and all data were collected through recording and transcription. Once the data was collected, a descriptive analysis of the interview results was conducted to describe how information security policies and procedures are implemented in the field. This analysis included categorizing the data based on ISO 27001:2022 control categories and identifying conformance with the standard and potential areas for improvement. The data in this study consists of primary data, in the form of interviews with informants, as well as secondary data from internal organizational documents and various literature sources, including books, journals, and relevant articles.

Results

Table 2 shows the results of interviews conducted at the BPJS Kesehatan Tondano Branch Office regarding implementing the Information Security Management System (ISMS). These interviews were guided by the ISO/IEC 27001:2022 control categories, covering four main areas: organizational control, people control, physical control, and technology control. Each table outlines key implementation aspects, the involved interviewees, and specific security practices adopted within the institution.

Table 2. Interview Results Related to ISMS Implementation at BPJS Kesehatan Tondano Based on ISO/IEC 27001: 2022 Control Categories

No	Category	Implementation Aspect	Interviewee	Description
1	Organizational Control	Policies for information security, Information security roles and responsibilities, Documented operating procedures	ISMS Officer Head of Information Technology	BPJS Kesehatan Tondano refers to ISO/IEC 27001:2022, internal guidelines, and legislation in its ISMS planning and documentation.
2	Organizational Control	Access Rights	ISMS Officer Head of Information Technology	System owners must review access rights annually and ensure they align with business needs and information security requirements.
3	Organizational Control	Access Rights	ISMS Officer Information Technology Officer	Granting or revoking access rights is based on official requests and implemented by authorized personnel.
4	Organizational Control	Authentication Information and Rights	ISMS Officer Head of Information Technology	Passwords must be changed regularly and not stored in automatic login systems.
5	People Control	User Identification and Authentication	Information Technology Officer Human Resources Officer	Employees are identified before accessing systems, and their authenticity is ensured through security guidelines, such as password policies. Users must change their default password upon initial system access, and passwords must be updated at least once every three months.
6	People Control	Password Guidelines and Integrity Pact	Human Resources Officer	Employees sign an ISMS and Integrity Pact.
7	Physical Control	Facility Access Control	Technology Information Officer Human Resources Officer	Access to work areas is restricted to authorized personnel who must present identity cards; visitors must be accompanied by authorized staff.

No	Category	Implementation Aspect	Interviewee	Description
8	Physical Control	Server Room Security	Information Technology Officer	The server room is locked when unattended and protected by identity verification systems, including ID cards and fingerprint recognition.
9	Physical Control	Surveillance and Alarms	Information Technology Officer	High-risk areas, such as server rooms, are monitored 24/7 with CCTV and alarms.
10	Technology Control	Mobile Device Security	Information Technology Officer Human Resources Officer	Laptops and smartphones must be password-protected and encrypted, especially when carrying internal FTP data.
11	Technology Control	Confidential Document Handling	Information Technology Officer Membership Staff	Digital files must be password-protected and encrypted; access is restricted to authorized personnel. Paper documents are manually destroyed.
12	Technology Control	Antivirus Usage	Information Technology Staff	All computers must have updated antivirus software; external devices cannot connect without it.

Source: data processed (2025)

As seen in the Table 2, implementing ISMS at BPJS Kesehatan Tondano is based on a structured and well-documented approach to meet ISO/IEC 27001:2022 standards. These interviews affirm that BPJS Kesehatan Tondano takes a proactive and comprehensive approach to ensuring its information systems' confidentiality, integrity, and availability.

Table 3 summarizes the interview results based on the four ISO/IEC 27001:2022 control categories. Most participants were not interviewed in all categories, because each control was only asked those with direct authority over its implementation. This was to maintain the relevance and accuracy of the data obtained during the interview process. This table reflects the relevance of each participant's area of responsibility to the information security control themes discussed.

Table 3. Summary of Interview Result

Theme	Description	Participant				
		1	2	3	4	5
Organizational Control	Policies for Information Security	✓	✓			
	Information Security Roles and Responsibilities	✓	✓			
	Documented Operating Procedures	✓	✓			
	Access Rights	✓	✓			
People Control	User Identification and Authentication			✓	✓	
	Password Guidelines and Integrity Pact			✓	✓	
Physical Control	Facility Access Control			✓	✓	
	Server Room Security			✓		
	Surveillance and Alarms			✓		
Technology Control	Mobile Device Security			✓		✓
	Confidential Document Handling			✓		✓
	Antivirus Usage			✓		

Source: data processed (2025)

The ISO/IEC 27001:2022 implementation matrix at the BPJS Kesehatan Tondano Branch is outlined in Table 4. It provides a structured overview of each control category, its purpose, supporting documents or regulations, and the organization's specific implementation practices. This matrix highlights how formal guidelines and internal regulations are applied to maintain information security following international standards.

The Tondano BPJS Kesehatan Branch Office is one of BPJS Kesehatan's service units, which is essential in managing participant and health service provider data. Information security management is crucial due to the increasing complexity of data and operations. Implementing an Information Security Management System (ISMS) aims to protect data from threats and ensure the safe and reliable operational sustainability.

The Tondano BPJS Kesehatan Branch Office has carefully designed, implemented, and maintained an Information Security Management System (ISMS). The ISMS planning process includes references to ISO/IEC 27001:2022, as well as other standards, the BPJS Kesehatan Internal Guidelines, and Legislation referred to by BPJS Kesehatan.

The Directorate of Information Technology's 2024 BPJS Kesehatan ISMS Guidelines document clearly and in detail outlines the company's Information Security Management System (ISMS). The guidelines serve as a reference for implementing information security principles, as directed by the BPJS Kesehatan Board of Directors.

BPJS Kesehatan plans, implements, evaluates, and improves its information security management performance based on ISO 27001:2022, which encompasses four key controls: organizational control, people control, physical control, and technology control. The implementation of the ISMS at the Tondano BPJS Kesehatan Branch Office is evident in the access control measures that have been carried out. Specifically, the company prohibits unauthorized users from accessing information, networks, and services. Based on the results of interviews with Tondano BPJS Kesehatan Branch Office staff, the owner of each system and facility requiring Special Access Rights must review, at least once a year, whether the access rights granted are still necessary for business needs and information security. Each review must be recorded and stored. The technical implementation of granting or revoking access rights is carried out by authorized personnel. These personnel do not have the authority to add or revoke access rights freely, but must be based on an official request from BPO (Business Process Outsourcing).

To mitigate the risk of unauthorized access to sensitive information, employees who access information and information systems must be correctly identified to ensure that only authorized personnel can access it. The company will also ensure that the authenticity of this information is maintained through robust information security provisions. The guidelines for using passwords such as passwords must not be known to others, including management and system administrators, the initial password must be changed when first entering the system, the password must be changed a maximum of 3 (three) months, or if there is a suspicion that the password has been spread, the password must not be stored in the automatic login system. Each employee will also sign the ISMS and Integrity Pact to maintain the confidentiality of the password.

Table 4. ISO 27001:2022 Implementation Matrix: BPJS Kesehatan Tondano Branch

Category Control	Description	Documents/ Regulations	Implementation at BPJS Kesehatan Tondado
Organizational Control	Controls that govern actions towards data protection, such as policies, rules, processes, procedures, and organizational structures.	Board of Directors Regulation No. 4 of 2024, BPJS Kesehatan ISMS Guidelines	1. The board of Directors provides ISMS guidance, there is a clear division of roles and responsibilities, and top management is committed to information security. 2. Evaluation of user access at least once a year by the system owner. 3. All access change requests must go through BPO 4. Has conducted periodic Internal Audits
People Control	Controls that organize the human components in interacting with data and each other	Board of Directors Regulation No. 4 of 2024, BPJS Kesehatan ISMS Guidelines	1. All employees must sign the Integrity Pact Form. 2. Each employee used a verified ID card and fingerprint to access information. 3. Passwords are not saved automatically and are only known to the owner. 4. Each password uses a combination of characters, is changed every 60 days, and does not use three previous passwords.
Physical Control	Controls that govern the security of physical assets to safeguard confidential information.	Board of Directors Regulation No. 4 of 2024, BPJS Kesehatan ISMS Guidelines. IT Standards Operational Procedure	1. All high-risk areas, such as server rooms and backup storage rooms, have 24-hour surveillance cameras and alarm systems. 2. Access to the server room is limited exclusively to authorized personnel who have completed identity verification procedures, including electronic ID cards and fingerprint authentication. 3. Unavailability of a paper shredder to destroy confidential physical documents
Technology Information Control	Controls that govern the security of information systems and networks using technological tools and procedures.	Board of Directors Regulation No. 4 of 2024, BPJS Kesehatan ISMS Guidelines. IT Standards Operational Procedure	1. Data backup is done regularly, tested every 3 months, and stored on separate media. 2. Mandatory antivirus on all devices, including BYOD and external parties. 3. Mobile devices must have encryption, password protection, and secure storage.

Source: data processed (2025)

The implementation of physical and environmental security is demonstrated by the company's issuance of identity cards to employees, contractors, and consultants, allowing them to access the BPJS Kesehatan work area. Access to facilities is restricted to authorized personnel only. Entry to restricted areas is only allowed for legitimate business or technical reasons. BPJS Kesehatan employees are required to accompany visitors to secure areas. The BPJS Kesehatan Tondano Branch Office server room will be locked if not guarded and protected from unauthorized and unwanted access. Physical security at BPJS Kehatan is implemented by restricting authorized access to the server room, which is only granted after identity verification procedures, including electronic identity cards and fingerprint recognition. All high-risk areas, including server rooms and backup storage rooms, have 24-hour surveillance cameras and alarm systems.

Mobile computing devices encompass laptops, mobile phones, smartphones, and tablet PCs, facilitating data storage, processing, and transfer. These devices are permitted only for the organization's main tasks. Mobile computing devices carrying internal FTP (File Transfer Protocol) information must meet the following requirements: a) Physical storage in a secure and locked condition, b) Laptops must be secured with a user and password and must be in a locked condition (screen lock), (c) If possible, laptops are integrated with a centralized directory system (active directory/LDAP). Laptops, tablets, and mobile phones containing confidential files related to BPJS operations must be password-protected, and internal storage media must be encrypted.

Important documents, including paper files and digital records, are stored safely. Paper documents are stored in a room inaccessible to the public and can only be moved into or out of the organization by trusted people. Electronic documents must be password-protected when files are exchanged via FTP or short messages. For confidential documents, only authorized personnel to handle the documents can access the part of the information system where the documents are located, the part of the information system where the documents are stored, and when files are exchanged via services such as FTP, short messages, and so on, they must be encrypted. Currently, the company lacks a paper shredder, resulting in the manual destruction of documents.

To prevent, ward off, and reduce the risk of viruses entering, every computer owned by BPJS Kesehatan is equipped with regularly maintained antivirus software. Computers owned by BPJS Kesehatan and personal computers used on behalf of the organization (Bring Your Device/BYOD) must use antivirus software approved by the corporation to detect and repair damage caused by malicious code. All computer devices owned by external parties that connect to the BPJS Kesehatan data communication network must have the latest version of antivirus software installed. If an external party's computer lacks antivirus protection or has an outdated version, it cannot connect to the BPJS Kesehatan data communication network.

Each work unit must regularly back up essential data related to the activities of all BPJS Kesehatan employees. If the data is not managed through an information system, the responsibility for data backup lies with the Deputy for Information Technology Operations.

Data backups must be conducted on media different from the primary media used for operations. Backups that contain confidential information, such as master files, employee personal information, salary details, individual health service data, and internal audit results, stored on portable media, must be secured and encrypted. Additionally, every data backup must be tested at least once every three months. This testing involves performing a data restoration process on the device to ensure all data is restored. The restoration process for the primary database should be carried out simultaneously with the restoration of secondary data (DRC).

Discussion

Organizational Control Implementation

The core of the organizational control framework at the BPJS Kesehatan Tondano Branch is the principle of least privilege. This fundamental cybersecurity concept dictates that individuals and systems are granted only the minimum level of access and permissions necessary to perform their specific job functions. By strictly adhering to this principle, as outlined in ISO 27001:2022, the organization systematically minimizes its attack surface. The logic is straightforward: the fewer people who have access to sensitive information or critical systems, the lower the probability of accidental data leaks or malicious misuse. This selective limitation of access is a proactive and highly effective risk mitigation strategy, which is critical in a sector that handles vast amounts of confidential personal and medical data (Apeh et al, 2023).

The practical application of this principle is managed through a meticulously structured access rights management policy. This policy is governed by formal procedures that ensure all requests for access, whether for new employees or for a change in role, are officially documented and approved. The process begins with a formal request from the user's manager, known as the Business Process Owner (BPO), which justifies the need for specific access rights based on an employee's responsibilities. To ensure the long-term integrity of this system, the organization conducts regular, often annual, access reviews. During these evaluations, all access rights are reassessed to confirm that they remain consistent with current business needs. This continuous monitoring is crucial, as it helps to identify and revoke permissions for employees who have changed roles or left the organization, thereby preventing the accumulation of unnecessary and risky access rights. While this framework is robust, its long-term effectiveness hinges on continuous vigilance and adaptation to evolving organizational structures and technological landscapes.

Human Capital and Behavioral Challenges

A significant and often underestimated barrier to a successful ISMS implementation is not technological but human. The most formidable challenge is employee resistance to changes in established information security policies. Security is an endeavor to protect a company's information assets from all potential threats (Kornelia & Irawan, 2021). However, employees who are accustomed to less restrictive work environments may perceive new security protocols as burdensome, time-consuming, or an impediment to their productivity.

In an effort to overcome this inertia, the Tondano BPJS Kesehatan Branch has taken critical initial steps, including requiring employees to sign an integrity pact and conducting socialization sessions about the ISMS. While these actions are commendable and necessary, they represent only the beginning of a long-term cultural transformation. A signed document or a single training session, while symbolic, is insufficient to embed a deep-seated security consciousness. To bridge this gap, more intensive and continuous efforts are needed in training and communication. The organization must move beyond simply informing employees and focus on educating and empowering them. This includes providing regular, tailored training sessions on topics like phishing awareness, secure password practices, and data handling protocols. Communication should be a two-way street, where employees are encouraged to report potential security issues without fear of reprisal.

Ultimately, the success of the ISMS depends on the cultivation of an organizational culture that is inherently adaptive to information security principles. This requires a fundamental shift in mindset, from viewing security as the sole responsibility of the IT department to understanding it as a collective, shared obligation. Management plays a pivotal role in this transformation by not only enforcing policies but also serving as role models and champions of security awareness. The implementation of role-based access control and strict identity verification policies underscores the importance of individual accountability for access rights. However, for these controls to be truly effective, they must be reinforced through consistent performance evaluations and ongoing coaching. When security awareness is integrated into performance metrics and becomes an integral part of the work culture, it ceases to be a mere policy and becomes a core value, thereby significantly strengthening the organization’s overall security posture.

Physical Control Implementation

The physical controls at the Tondano BPJS Kesehatan Branch are a strong complement to its digital security measures. The implementation of safeguards such as limiting access to work areas using electronic identity cards and securing server rooms with a fingerprint verification system are in full compliance with the physical security standards set by ISO 27001. Biometric authentication, in particular, offers a robust and highly secure method of controlling entry, as it uses unique biological characteristics to prevent unauthorized access. The fingerprint system for the server room is a critical barrier, ensuring that only authorized personnel can enter an area containing the organization’s most vital hardware and data.

However, a notable and critical weakness was identified in the absence of a paper shredder for the destruction of confidential documents. While the focus on digital security is paramount in the modern era, physical information security remains equally important. Documents containing sensitive personal information, financial data, or internal strategies pose a significant risk if not disposed of properly. Merely throwing them into a waste bin makes them susceptible to dumpster diving or unauthorized retrieval. A paper shredder provides a simple yet crucial layer of defense by permanently destroying physical documents, thereby preventing the misuse of sensitive information. Beyond its security benefits, implementing paper shredders also supports environmental sustainability by facilitating the proper disposal of paper, reducing the practice of burning paper waste that contributes to climate change (Zendrato & Zarlis, 2018). The addition of this facility is therefore not just a matter of enhancing physical security but also of ensuring full compliance with internal BPJS Kesehatan guidelines and promoting responsible environmental practices.

Technology Information Implementation

From a technological standpoint, the Tondano BPJS Kesehatan Branch demonstrates a clear commitment to data protection. The implementation of security technologies such as centralized antivirus, data encryption on mobile devices, and regular data backup procedures showcases the organization's dedication to maintaining data integrity and confidentiality. Centralized antivirus ensures that all network endpoints are protected from malicious software, with updates and scans managed from a single point. Data encryption on mobile devices is vital for protecting sensitive information that is often accessed outside the secure network perimeter, safeguarding it from theft or loss. Regular data backups are a cornerstone of any disaster recovery plan, ensuring that the organization can restore its data and operations in the event of a system failure, cyberattack, or natural disaster.

Despite these strong foundational controls, the organization faces significant resource limitations, both in its technological infrastructure and human capital. These limitations pose a formidable challenge to maintaining the continuity and effectiveness of these technical controls. For example, the organization may need to more effectively manage Bring Your Own Device (BYOD) policies, which introduce a complex array of security risks due to the varying levels of security on personal devices. The current infrastructure may also lack the necessary capacity and resilience for backup systems, making it vulnerable to large-scale data loss in the event of a catastrophic failure. Upgrading backup systems to include redundant, off-site storage and higher capacity is essential for ensuring business continuity and data resilience.

Conformance and Strategic Recommendations for Improvement

The BPJS Kesehatan Tondano Branch's ISMS implementation, guided by ISO/IEC 27001:2022, represents a strategic move to align with a global standard designed to address cybersecurity challenges and build digital trust (Malatji, 2023). This conformance demonstrates the organization's commitment to excellence and to protecting its stakeholders. However, compliance is not a static endpoint but a continuous journey. To ensure that policy implementation is not a mere formality, the organization must prioritize continuous evaluation and internal audits. These periodic reviews are crucial for identifying vulnerabilities, addressing emerging threats, and ensuring that security controls remain effective and relevant.

In light of the identified resource limitations and challenges, several recommendations are proposed for future improvement. First, management must make a strategic investment to enhance technological capacity. This includes upgrading network infrastructure, investing in more advanced security technologies, and acquiring the necessary hardware and software to support a more resilient backup system. Second, the organization must strengthen its training and socialization programs to move beyond basic awareness and foster a deep-seated information security culture. This can be achieved through regular, interactive workshops, simulations, and the integration of security awareness into performance metrics. A proactive approach to overcoming these barriers will not only increase the organization's resilience in the face of escalating cybersecurity risks but will also solidify stakeholder trust, confirming its position as a responsible and reliable public service provider.

Conclusion

The Tondano BPJS Kesehatan Branch Office has demonstrated the implementation of an excellent and structured Information Security Management System (ISMS), consistently referencing the ISO/IEC 27001:2022 standard and internal organizational guidelines. Access rights management is carried out through strict, formal procedures, including periodic evaluations of access and applying the principle of least privilege, which reflects high compliance with organizational controls. This indicates that information security governance has been carried out correctly and is accountable.

In addition, physical security and the application of information technology, such as biometric identification systems, CCTV monitoring, centralized antivirus, device encryption, and data backup procedures, demonstrate solid technical and operational readiness in maintaining information confidentiality and integrity. Although there are still some minor obstacles, such as the unavailability of physical document shredders, limited infrastructure resources, and human resource behavioral challenges, these do not detract from the overall quality of implementation.

Overall, this achievement demonstrates that the Tondano BPJS Kesehatan Branch Office is on the right track in implementing ISMS. With continuous improvement in resource allocation and strengthening of organizational culture, the effectiveness of information security management can continue to be enhanced to meet regulatory demands and the evolving dynamics of risks.

References

Apeh, A. J., Hassan, A. O., Oyewole, O. O., Fakeyede, O. G., Okeleke, P. A., & Adaramodu, O. R. (2023). GRC strategies in modern cloud infrastructures: A review of compliance challenges. *Computer Science & IT Research Journal, 4*(2), 111–125.

Drljača, D., & Latinović, B. (2016). Frameworks for audit of an information system in practice. *JITA-APEIRON, 12*(2).

Jannah, M., Hidayat, M. F., Agustiyyani, M., Buana, P. W., & Purwani, F. (2024). Implementasi Autentikasi Biometrik untuk Meningkatkan Keamanan dan Privasi Pengguna Dompet Digital. *Journal of Scientech Research and Development, 6*(2), 531-539.

Fatih, D., & Aji, R. F. (2024). Evaluasi Keamanan Informasi Menggunakan ISO/IEC 27001: Studi Kasus PT XYZ. *J-SAKTI (Jurnal Sains Komputer dan Informatika), 8*(1), 72-84.

Fauzi, R. (2018). Implementasi Awal Sistem Manajemen Keamanan Informasi pada UKM Menggunakan Kontrol ISO/IEC 27002. *JTERA (Jurnal Teknologi Rekayasa), 3*(2), 3.

Kornelia, A., & Irawan, D. (2021). Analisis keamanan informasi menggunakan tools Indeks Kami ISO 4.1. *Jurnal Pengembangan Sistem Informasi dan Informatika, 2*(2), 78–86.

Lambi, M. (2023). *Sistem Informasi Manajemen AI (Artificial Intellegent) as the Future Management System*. Uwais Inspirasi Indonesia.

Lenawati, M., & Winarno, W. W. (2017). Tata Kelola Keamanan Informasi Pada PDAM Menggunakan ISO/IEC 27001: 2013 Dan Cobit 5. *Speed-Sentra Penelitian Engineering dan Edukasi, 9*(1).

Malatji, M. (2023). Management of enterprise cyber security: Areview of ISO/IEC 27001:2022. *International Conference on Cyber Management And Engineering (CyMaEn)*, 117–122.

Pamungkas, W. C., & Saputra, F. T. (2020). Evaluasi Keamanan Informasi Pada SMA N 1 Sentolo Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001: 2013. *Jurnal Sistem Komputer dan Informatika (JSON), 1*(2), 101-106.

Paramita, S., Siregar, S. A., Damanik, R. A., & Irawan, M. D. (2022). Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001: 2013. *Bulletin of Information Technology (BIT), 3*(4), 374-379.

Prawiranata, R. T. A. (2024). Sistem Manajemen Keamanan Informasi (SMKI) di PT. Surveyor Indonesia Cabang Surabaya: Penerapan Standar ISO 27001: 2013. *ULIL ALBAB: Jurnal Ilmiah Multidisiplin, 3*(6), 105-112.

Pujiani, F., & Bisma, R. (2024). Strategi Optimalisasi Manajemen Konfigurasi untuk Keamanan Informasi Berdasarkan ISO/IEC 27001: 2022. *Journal of Emerging Information System and Business Intelligence (JEISBI), 5*(3), 223-228.

Sinaga, R. (2023). Pengembangan Model Penilaian Kepatuhan Salah Satu Perguruan Tinggi Terhadap Standar ISO 27001: 2022. *Jurnal Teknik Informatika dan Sistem Informasi, 9*(3), 381-394.

Soesanto, E., Kurniasih, F., Mutiara, P., & Afifi, S. T. (2023). Sistem manajemen keamanan informasi dengan standar ISO/IEC 27001 dan ISO/ICE 27002 pada PT Jasa Marga. *Co-Creation: Jurnal Ilmiah Ekonomi Manajemen Akuntansi dan Bisnis, 1*(4), 169-179.

Suryono, I. (2023). Isms Evaluasi Penilaian Mandiri Penerapan SMKI Di Lingkungan Lembaga Awdx: Evaluasi implementasi SMKI. *JUPIK: Jurnal Penelitian Ilmu komputer, 1*(1).

Winanti, M. B., & Dzulhan, I. (2018). Audit Keamanan Sistem Informasi Akademik Dengan Kerangka Kerja ISO 27001 Di Program Studi Sistem Informasi Unikom. *Majalah Ilmiah Unikom, 16*(2), 121-131.

Tim Redaksi BSSN. (2022). *Lanskap Keamanan Siber Indonesia 2022*. Badan Sandi Dan Siber Negara.

Yustanti, W., Bisma, R., Qoriah, A., & Prihanto, A. (2018). *Keamanan Sistem Informasi*. Sidoarjo: Zifatama Jawara.

Zendrato, N., & Zarlis, M. (2018). Analisis Keamanan Data Dengan Pengformatan Media Penyimpanan Dengan Metode OS Format Dan Low Level Format. *Prosiding Seminar SeNTIK, 2*(1), 146-151.