Journal of Computer, Information and Technology Vol: 6, No. 1, 2026, Page: 1-18

Implementation of ISO/IEC 27001:2013 for Information Security Management System at Information System Unit of PT. KAI Divre III Palembang

Irvan Ramadhan, Nyimas Sopiah*

Universitas Bina Darma

DOI: https://doi.org/10.53697/jkomitek.v6i1.3749
*Correspondence: Nyimas Sopiah
E-mail: nyimas.sopiah@binadarma.ac.id

Received: 22-04-2026
Accepted: 22-05-2026
Published: 22-06-2026

Abstract: The background of this research is the vulnerability of the Information System Unit of PT KAI Divre III Palembang to cyber threats such as malware, saved browser passwords, and weak physical asset management, amidst high dependence on IT for transportation operations. The purpose of the research is to analyze the condition of the ISO/IEC 27001:2013-based ISMS, identify gaps, and recommend controls through the PDCA cycle. This type of research is a qualitative descriptive study with a case study approach. The population is all unit personnel (15 people), a sample of 10 key informants via purposive sampling. Instruments include semi-structured interviews, checklist observations, and document analysis) (analysis techniques use the Miles and Huberman model with a gap and risk matrix. The results show that the implementation of PDCA is effective: high risks (malware, fire extinguishers) and medium risks are reduced to low through antivirus, device locking, inventory updates, and time synchronization audit corrections. The conclusion is that the ISMS has been structured, increasing operational resilience, although further quantitative evaluation is needed.

Keywords: Information Security, Iso 27001, Pdca Cycle, Risk Assessment, Smki

Introduction

The rapid development of information technology has driven organizations, including state-owned enterprises like PT KAI, to increasingly rely on information systems to support business operations, decision-making, and public services. However, this dependence also increases information security risks such as data leaks and system disruptions. Therefore, information, as a strategic asset, requires systematic management to maintain its confidentiality, integrity, and availability (Ritzkal et al, 2019) (Susanto & Almunawar, 2021). PT KAI Divre III Palembang, through its Information Systems Unit, manages crucial IT infrastructure for the South Sumatra region, but remains vulnerable to external and internal threats in this digital era (Damanik et al, 2023) (Riana et al, 2023).

The Information Systems Unit of PT KAI Divre III Palembang is facing a growing global cyber threat affecting the transportation sector, with malware attacks and unauthorized access frequently disrupting operations. This phenomenon is exacerbated by the reliance on information systems for ticketing and train operational data, which require multiple layers of protection to maintain reliable public services (Alreemy et al, 2022) (Mesquida et al, 2021).

The main problem arises from the threat of viruses and malware on work devices connected to the internal network, potentially causing system damage and data theft at the Information Systems Unit of PT KAI Divre III Palembang. The practice of using the save password feature in browsers is still common, increasing the risk of unauthorized access if the device falls into the hands of third parties (Ritzkal et al, 2019) (Kalaimannan et al, 2021). Furthermore, failing to lock devices when left unattended exacerbates vulnerabilities, opening up opportunities for misuse of sensitive information (Damanik et al, 2023) (Siponen et al, 2022).

Physical issues include IT asset inventories that are not regularly updated, complicating oversight and risking asset loss. Hot server room temperatures threaten hardware stability, while expired fire extinguishers indicate weak environmental controls, all of which compromise information availability (Riana et al, 2023) (Fernandez et al, 2024). Without systematic management, these issues can result in operational downtime and financial losses for PT KAI (Goel & Shawky, 2021) (Nugroho et al, 2023).

Others include a lack of user awareness of basic safety procedures and irregular inventory updates, which weaken the unit's overall risk controls. This reflects a gap between daily practices and international standards, requiring risk-based interventions to minimize impact (Ritzkal et al, 2019) (Damanik et al, 2023).

This study aims to analyze the current state of information security in the Information Systems Unit of PT KAI Divre III Palembang, identify the causal factors of problems such as malware and access management, and determine relevant ISO/IEC 27001:2013 controls for improvement. The urgency lies in protecting crucial information assets in the public transportation sector, preventing service disruptions that have a broad impact on the people of South Sumatra. The novelty of this study is the application of the PDCA cycle in ISO/IEC 27001:2013 specifically in an Indonesian regional transportation state-owned enterprise, complementing previous studies with practical recommendations based on actual gap analysis (Riana et al, 2023) (Susanto & Almunawar, 2021).

Methodology

This study uses a qualitative descriptive approach that aims to describe the overall implementation of the Information Security Management System (ISMS) based on ISO/IEC 27001:2013 at the Information Systems Unit of PT KAI Divre III Palembang. This descriptive research type was chosen because it focuses on presenting facts, phenomena, and existing information security practices in the field without testing hypotheses or causal relationships, making it suitable for analyzing the gap analysis of clauses and controls of Annex A of the international standard (Sugiyono, 2021) (Creswell & Poth, 2022). The qualitative approach allows for in-depth exploration of the organizational context, policies, procedures, and user behavior through narrative data, as applied in similar studies on ISMS implementation in the transportation sector and state-owned enterprises (SOEs) (Ritzkal et al, 2019) (Damanik et al, 2023).

The research instruments included semi-structured interview guidelines, an ISO/IEC 27001:2013 clause checklist-based observation sheet, and analysis documents such as

security policies, IT asset inventories, and internal audit reports collected from the Information Systems Unit of PT KAI Divre III Palembang. Data collection techniques included in-depth interviews with IT staff and management, direct observation of physical infrastructure and device operations, and document review to verify compliance with the PDCA cycle and Annex A controls, with data triangulation to enhance validity (Emzir, 2021) (Sudaryono, 2022). Data analysis techniques applied the Miles and Huberman interactive model, which includes data reduction, data display in the form of a gap analysis matrix and risk assessment, and drawing conclusions to formulate relevant security control recommendations, as used in previous ISMS evaluations (Riana et al, 2023) (Creswell & Poth, 2022).

The study population consisted of all personnel of the Information Systems Unit of PT KAI Divre III Palembang, totaling approximately 15 people, including IT managers, network technicians, and asset administration staff, who are directly involved in infrastructure management and information security. The sample was determined through a purposive sampling technique with the criteria of key informants having at least two years of experience in IT operations and knowledge of security risks such as malware and access control, resulting in 10 key respondents to ensure comprehensive representation without ignoring the sensitive aspects of BUMN data (Sugiyono, 2021) (Sudaryono, 2022). This sample selection aligns with the principle of qualitative data saturation, where data collection is stopped when new information no longer emerges, as applied in ISO/IEC 27001 studies on similar organizations (Damanik et al, 2023) (Emzir, 2021).

The research procedure began with a preparatory phase consisting of an in-depth literature study on ISO/IEC 27001:2013, access permits through NDA, and the development of instruments based on clauses 4-10 and Annex A for gap analysis. The implementation phase included primary data collection through interviews, observations, and secondary data from documents for three months at the PT KAI Divre III Palembang location, followed by a risk analysis using a probability-impact matrix and PDCA mapping to identify non-conformities such as expired fire extinguishers and saved browser passwords. The final phase involved validating the findings through member checking and developing control implementation recommendations, ensuring a logical flow from condition description to sustainable solutions (Creswell & Poth, 2022) (Ritzkal et al, 2019).

Results and Discussion

Overview of Research Object

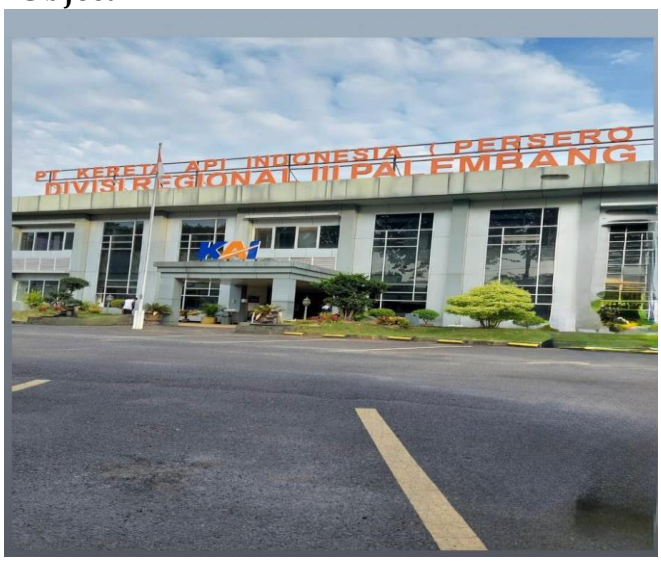


Figure 1. Palembang Division III Office

The object of this study is the Information Systems Unit of PT. Kereta Api Indonesia (Persero) Regional Division III Palembang. This unit plays a strategic role in supporting the smooth operation of the company through the provision, management, and maintenance of information systems and information technology infrastructure used in the company's business activities. The managed information systems include various operational applications, internal data processing, communication networks, and hardware and software management.

As a regional division of PT. KAI, Divre III Palembang is responsible for railway operations in South Sumatra and the surrounding area. In carrying out this responsibility, the Information Systems Unit ensures the availability of accurate, timely, and secure information. The high reliance on information technology makes information security a crucial aspect to prevent operational disruptions, data leaks, and other risks that could harm the company.

Description of Research Results

Based on the results of research conducted at the Information Systems Unit of PT. KAI Divre III Palembang, the implementation of the Information Security Management System (ISMS) using the Plan–Do–Check–Act (PDCA) method has been carried out well and in a structured manner. Each PDCA stage has been carried out systematically as part of the organization's efforts to meet the requirements of ISO/IEC 27001:2013 and maintain the security of its information assets. The results of the study indicate that the PDCA cycle has become the main framework in the planning, implementation, evaluation, and continuous improvement of the ISMS related to the ISO 270001 Clause.

PDCA Implementation Stages based on ISO 27001 Clauses

1. Plan Stage

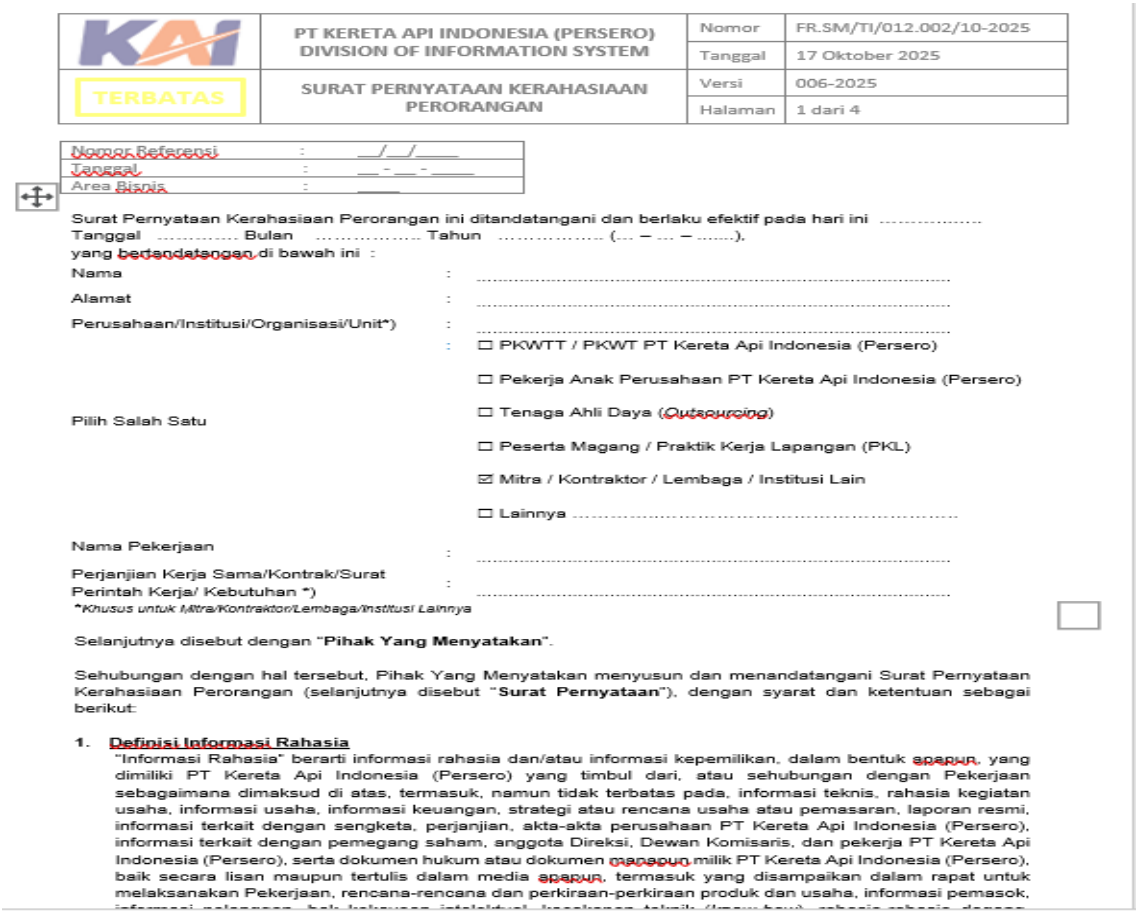
At the Plan stage, it relates to clauses 4 to 7. In Clause 4.1, understand the organizational context, both internally and externally, and its organizational structure.

A. Filling out a Non-Disclosure Agreement (NDA)

Filling out a Non-Disclosure Agreement (NDA) is a form of information security control implemented to protect the confidentiality of an organization's information from the risk of leakage or misuse. NDAs apply to both internal and external parties who have access to information and systems within the Information Systems Unit of PT Kereta Api Indonesia (Persero) Regional Division III Palembang.

Internally, NDAs are mandatory for all staff and employees involved in the management or use of information systems. Filling out an NDA serves to emphasize staff's obligation to maintain the confidentiality of information, both during and after they cease their employment with the organization. Through NDAs, staff understand the limitations of information use, their responsibilities for data security, and the consequences of breaches of confidentiality provisions.

Meanwhile, externally, NDAs are also required for parties with access to organizational information, such as interns and partners. Interns involved in operational or technical activities have the potential to access internal data and systems, so they need to be provided with an understanding and written commitment to maintain the confidentiality of information obtained during the internship. Similarly, for partners, NDAs serve as a legal basis and administrative control to ensure that organizational information is not used beyond the agreed-upon purposes of the collaboration. This policy also includes sanctions for violators, ranging from warnings to legal action in accordance with applicable regulations.



	PT KERETA API INDONESIA (PERSERO) DIVISION OF INFORMATION SYSTEM	Nomor	FR.SM/TI/012.002/10-2025
		Tanggal	17 Oktober 2025
TERBATAS	SURAT PERNYATAAN KERAHASIAAN PERORANGAN	Versi	006-2025
		Halaman	1 dari 4

Nomor Referensi	:	__/__/____
Tanggal	:	__ - __ - ____
Area Bisnis	:	____

Surat Pernyataan Kerahasiaan Perorangan ini ditandatangani dan berlaku efektif pada hari ini ……
Tanggal …… Bulan …… Tahun …… (… – … – ……).
yang bertandatangan di bawah ini :

Nama : ……

Alamat : ……

Perusahaan/Institusi/Organisasi/Unit*) : ……

Pilih Salah Satu :

☐ PKWTT / PKWT PT Kereta Api Indonesia (Persero)

☐ Pekerja Anak Perusahaan PT Kereta Api Indonesia (Persero)

☐ Tenaga Ahli Daya (*Outsourcing*)

☐ Peserta Magang / Praktik Kerja Lapangan (PKL)

☑ Mitra / Kontraktor / Lembaga / Institusi Lain

☐ Lainnya ……

Nama Pekerjaan : ……

Perjanjian Kerja Sama/Kontrak/Surat Perintah Kerja/ Kebutuhan *) : ……

**Khusus untuk Mitra/Kontraktor/Lembaga/Institusi Lainnya*

Selanjutnya disebut dengan "**Pihak Yang Menyatakan**".

Sehubungan dengan hal tersebut, Pihak Yang Menyatakan menyusun dan menandatangani Surat Pernyataan Kerahasiaan Perorangan (selanjutnya disebut "**Surat Pernyataan**"), dengan syarat dan ketentuan sebagai berikut:

1. **Definisi Informasi Rahasia**
   "Informasi Rahasia" berarti informasi rahasia dan/atau informasi kepemilikan, dalam bentuk apapun, yang dimiliki PT Kereta Api Indonesia (Persero) yang timbul dari, atau sehubungan dengan Pekerjaan sebagaimana dimaksud di atas, termasuk, namun tidak terbatas pada, informasi teknis, rahasia kegiatan usaha, informasi usaha, informasi keuangan, strategi atau rencana usaha atau pemasaran, laporan resmi, informasi terkait dengan sengketa, perjanjian, akta-akta perusahaan PT Kereta Api Indonesia (Persero), informasi terkait dengan pemegang saham, anggota Direksi, Dewan Komisaris, dan pekerja PT Kereta Api Indonesia (Persero), serta dokumen hukum atau dokumen manapun milik PT Kereta Api Indonesia (Persero), baik secara lisan maupun tertulis dalam media apapun, termasuk yang disampaikan dalam rapat untuk melaksanakan Pekerjaan, rencana-rencana dan perkiraan-perkiraan produk dan usaha, informasi pemasok,

Figure 2. NDA Letter

Thus, NDA not only functions as an administrative measure, but also as an information security control that complies with the provisions of ISO/IEC 27001:2013, particularly clause A.7.2.2: Confidentiality agreements, which emphasizes the importance of confidentiality agreements for all personnel who have access to sensitive information.

B. Organizational structure

The Information Systems Unit of Regional Division III Palembang is headed directly by a Manager and has three Assistant Managers. It also has three Executives and is assisted by eight outsourced personnel.

Figure 3. Organizational Structure

From the picture, the manager is colored green, the assistant manager blue, the executor black, and the outsourcing white. The IT Unit's boundaries extend from Kertapati to Lubuk Linggau, including the Regional Division office, STC Training Center, the Regional Transportation Center, and the Palembang LRT. The area map is as follows:

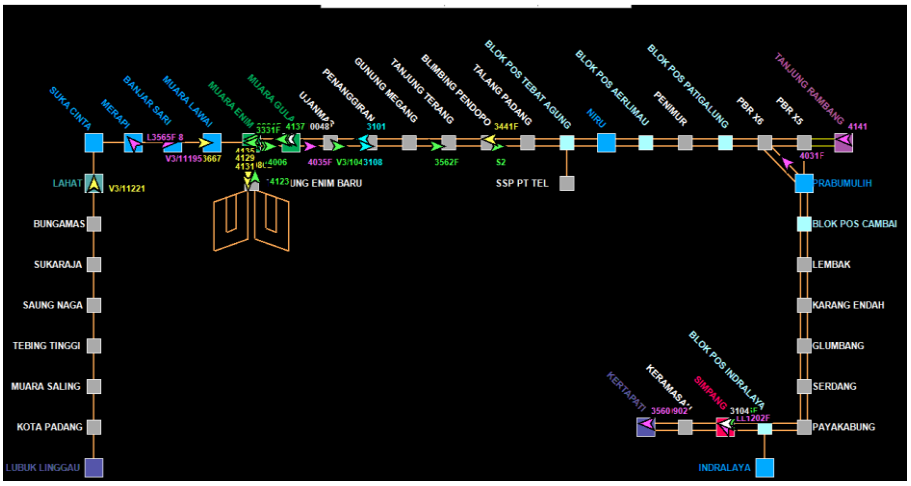


Figure 4. Regional Map

From the image, there are 31 active stations which have large stations including Kertapati, Prabumulih, Muaraenim, Lahat, and Lubuk Linggau stations.

Clause 5.2 outlines the roles, responsibilities, and authority of the organization. In the context of the Palembang Regional Division III Information Systems Unit, the implementation of Clause 5.2 can be understood through the existing organizational structure and division of roles. This unit is led directly by a Manager who has primary responsibility as the highest authority in managing and controlling information systems in the Palembang Regional Division III area.

The Manager is assisted by three Assistant Managers who act as liaisons between strategic policies and operational implementation. The Assistant Managers are responsible for coordinating technical and administrative activities, ensuring that information security controls are implemented according to procedures, and overseeing the performance of the implementation team. At this level, authority is delegated in a controlled manner to ensure operational processes remain effective without neglecting information security aspects.

Furthermore, there are three Implementers directly responsible for the day-to-day operational activities of the information system. Implementers carry out technical tasks such as managing IT devices, systems, and services, and implementing information security controls in accordance with established policies and directives. They play a critical role in maintaining the confidentiality, integrity, and availability of information at the operational level.

To support these activities, the Information Systems Unit of Regional Division III Palembang is also assisted by eight outsourced personnel. These outsourced personnel act as operational support, with clearly defined scopes of duties and authorities defined through work agreements. In accordance with Clause 5.2, the roles and responsibilities of outsourced personnel must be clearly understood and limited as needed to minimize information security risks.

Clause 6.1 on Actions to Address Risks and Opportunities requires organizations to identify risks and opportunities related to information security that need to be addressed. Information security risks arise from threats, vulnerabilities, and impacts on the organization's information assets. Therefore, organizations are required to conduct a structured information security risk assessment to identify potential risks that could compromise the confidentiality, integrity, and availability of information.

A risk assessment matrix is a tool used to determine risk levels based on a combination of the likelihood of a risk occurring and the impact if it occurs. This matrix helps organizations systematically and objectively identify risk management priorities, particularly in the implementation of information security risk management. The following is a matrix table for calculating risk scores.

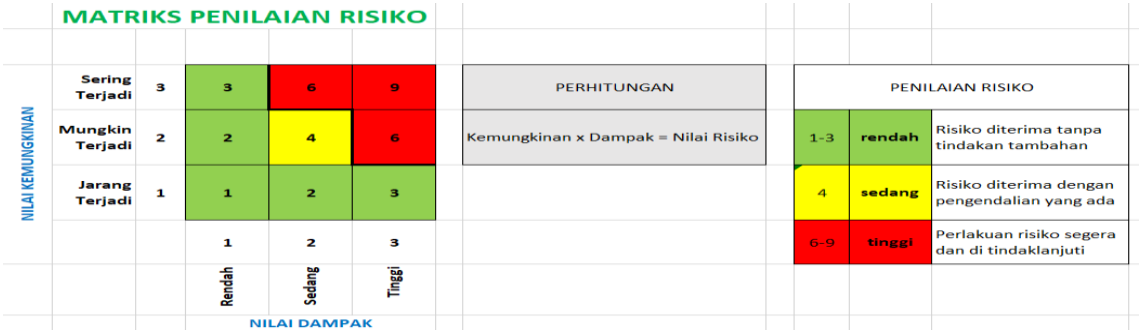


Table 5. Risk Assessment Matrix

In the matrix, the vertical line shows the probability value, which consists of three levels: rare with a value of 1, likely with a value of 2, and frequent with a value of 3. The higher the value, the greater the chance of the risk occurring. Meanwhile, the horizontal line shows the impact value, which is also divided into three levels: low with a value of 1, medium with a value of 2, and high with a value of 3. Impact describes the magnitude of the risk's influence on operations, information security, or organizational goals.

The risk value is obtained by multiplying the probability value by the impact value (Risk = Probability × Impact). This calculation produces a risk value between 1 and 9. This value is then mapped to a risk category indicated by a color in the matrix, making it easier to visualize the risk level.

Low risk categories are indicated by the color green and have a value between 1 and 3. Risks in this category are acceptable to the organization without requiring additional action, but regular monitoring is still required. Furthermore, moderate risks are indicated by the color yellow with a value of 4, meaning the risk is still acceptable but must be managed through existing controls or limited improvements. High risks are indicated by the color red with a value of 6 to 9, which indicates the risk must be immediately addressed and followed up with appropriate mitigation actions. The following table shows the identified risk assessments.

Penilaian Resiko Keamanan Informasi					
No	**Risiko**	**Level Kemungkinan**	**Level Dampak**	**Penilaian Risiko**	**Keterangan / Tindakan**
1	Ancaman serangan virus dan malware pada perangkat kerja	2	3	6 – Tinggi	Perlakuan risiko segera: install antivirus dan update rutin
2	Mengaktifkan fitur penyimpanan kata sandi (save password) pada browser	2	2	4 – Sedang	Risiko diterima dengan pengendalian: Menonaktifkan fitur penyimpanan kata sandi pada browser
3	Kelalaian pengguna dalam mengamankan perangkat	2	2	4 – Sedang	Risiko diterima dengan pengendalian: penguncian perangkat dan penyimpanan perangkat di tempat aman
4	Data inventaris aset TI belum diperbarui	2	2	4 – Sedang	Risiko diterima dengan pengendalian: pembaruan inventaris secara rutin dan kegiatan stock opname berkala
5	APAR yang sudah melewati masa berlaku	2	3	3 – Tinggi	Perlakuan risiko segera: cek dan ganti APAR, jadwal pemeriksaan rutin

Table 6. Risk Assessment

Based on the Information Security Risk Assessment table, it can be concluded that the Information Systems Unit still faces several risks that could potentially compromise information security and workplace safety. Of the five identified risks, two are considered high-level: the threat of viruses and malware attacks on work equipment and the expired

condition of fire extinguishers. These two risks require immediate risk management due to their significant impact on operations and safety, and must be addressed through consistent technical and preventive measures.

Meanwhile, three other risks are at a moderate level: the use of browser password storage features, user negligence in securing devices, and outdated IT asset inventory data. These risks are acceptable as long as the organization implements adequate controls, such as security policies, user education, and regular data and procedure updates.

Overall, the risk assessment results indicate that the organization has been able to identify and classify information security risks quite well. Once risks are identified, the organization must undertake information security risk treatment. This risk treatment can take the form of risk reduction through mitigation or corrective actions. The following table shows the mitigated risks.

PENANGGANAN RESIKO						
No	Risiko	Mitigasi / Tindakan Perbaikan	Dampak (Setelah)	Kemungkinan (setelah)	Nilai Resiko (Setelah)	Keterangan
1	Ancaman serangan virus dan malware pada perangkat kerja	Instal antivirus, update rutin	3	1	3	Risiko menurun ke tingkat rendah setelah antivirus diinstal dan pembaruan sistem secara rutin
2	Mengaktifkan fitur penyimpanan kata sandi (save password) pada browser	Nonaktifkan fitur save password	2	1	2	Risiko berhasil diturunkan ke tingkat rendah dengan menonaktifkan fitur penyimpanan kata sandi.
3	Kelalaian pengguna dalam mengamankan perangkat	Terapkan penguncian perangkat dan simpan perangkat di tempat yang aman	2	1	2	Risiko menjadi rendah setelah diterapkannya penguncian perangkat dan penyimpanan perangkat di tempat aman
4	Data inventaris aset TI belum diperbarui	Buat update rutin inventaris dan Lakukan Stock Opname setiap 6 bulan sekali	2	1	2	Risiko berada pada tingkat rendah setelah dilakukan pembaruan inventaris secara rutin dan kegiatan stock opname berkala
5	APAR yang sudah melewati masa berlaku	Ganti/isi ulang APAR segera, inspeksi rutin bulanan	3	1	3	Risiko berhasil diturunkan ke tingkat rendah setelah dilakukan penggantian atau pengisian ulang APAR serta inspeksi rutin bulanan

Table 7. Risk Management

Based on the Risk Management table, it can be concluded that all previously identified risks have been subject to appropriate mitigation and remedial measures. The assessment results indicate that the risk probability level has decreased to low (a value of 1) for all risks.

Overall, the risk management results indicate that the risk is at an acceptable level for the organization. Therefore, the organization has met the risk management principles as required in ISO/IEC 27001 Clause 6, specifically regarding the planning and implementation of actions to mitigate information security risks.

In implementing Subclause 7.3 of ISO/IEC 27001 Awareness, the Information Systems Unit of Regional Division III Palembang builds and improves information security awareness among all personnel involved in the management and use of information systems. This awareness is intended to ensure that each individual understands the importance of maintaining information security as a shared responsibility, not solely the responsibility of the information systems unit.

One of the main activities to raise information security awareness in the Information Systems Unit of Regional Division III Palembang was the online socialization of information security policies and procedures through the Zoom application. This activity was attended

by Managers, Assistant Managers, Implementers, and outsourced personnel involved in the management and use of information systems. The material presented included an understanding of information security policies, the roles and responsibilities of each personnel in maintaining the confidentiality and availability of information, as well as examples of frequently occurring information security risks, such as malware attacks, password leaks, and user negligence. Participants were also given reminders about basic security practices, such as locking work devices when not in use, not activating the save password feature on browsers, and the obligation to regularly update the system.

In addition to delivering the material, the Zoom socialization session also included discussions and a Q&A session, allowing participants to better understand the material and clarify any misunderstandings. Attendance was documented through screenshots of the activity as proof of implementation.

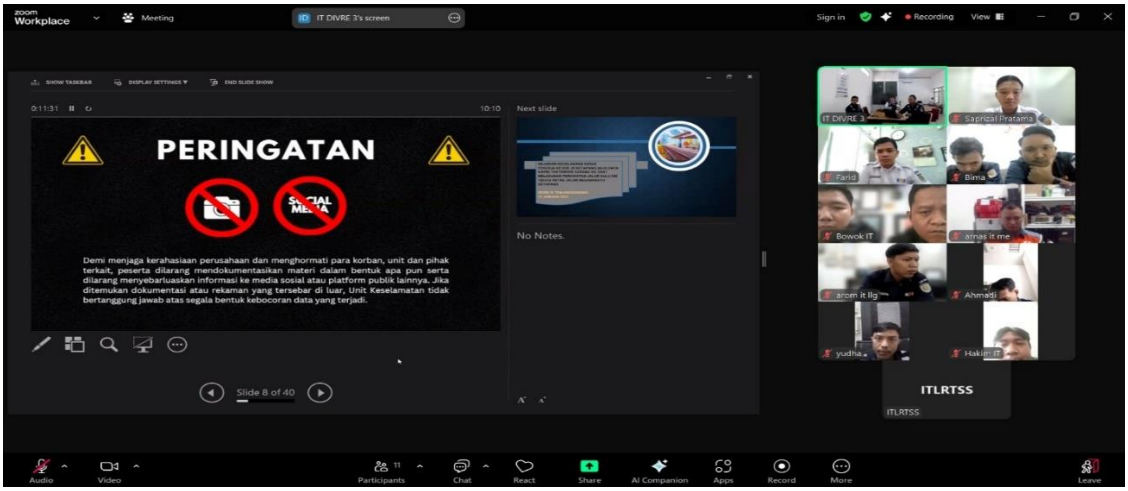


Figure 8. SMKI socialization

By implementing information security outreach using Zoom, the Palembang Regional Division III Information Systems Unit was able to effectively reach all personnel without being tied to a specific location, while ensuring that information security awareness was maintained and improved. This activity demonstrated the organization's commitment to consistently and documentedly meeting the requirements of ISO/IEC 27001 Clause 7.3.

2. Do (Implementation) Stage

At the Do stage related to Clause 8 of ISO/IEC 27001, Clause 8.3 Information Security Risk Treatment requires the organization to implement an Information Security Management System (ISMS) in real terms in accordance with the results of the risk assessment as set out in Clause 6.

A. Install antivirus

First, prepare the master installation of the Sentinel Agent antivirus, then install it on your laptop or computer device.

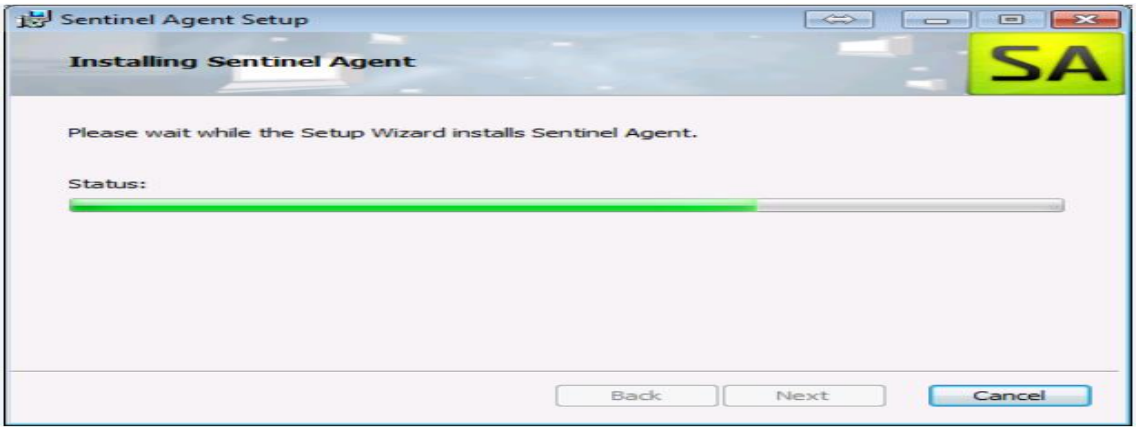


Figure 9. Antivirus Installation Process

After the installation process, a finish message will appear. Open the Sentinel application and make sure the update with the Last console connection time message matches the day and time when the application was opened.

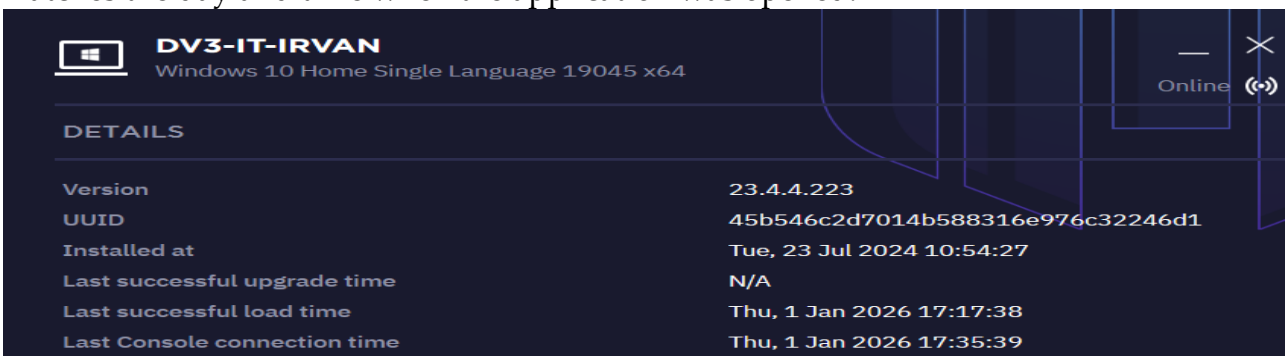


Figure 10. Antivirus Update

The last update showed the time January 1, 2026 at 5:17 PM on Thursday.

B. Disabling the Save Password Feature in the Browser

Open the Firefox application then select the settings menu in the security section, there is a description Ask to save passwords then deactivate the check mark on the menu as shown in the image below.

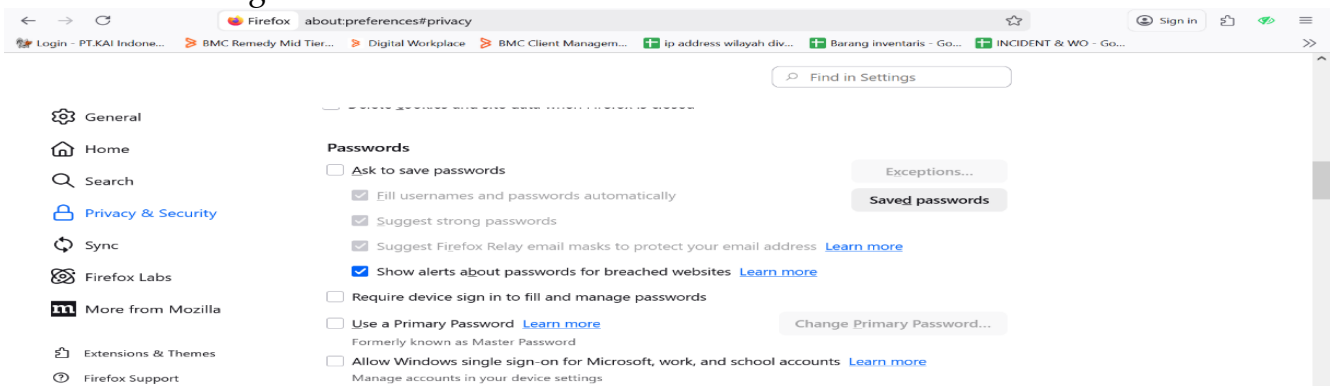


Figure 11. Disabling the Save Password Feature in the Browser

The save password feature on the browser has been disabled.

C. Lock the device and store it in a safe place

Open the control panel then select manage account then select create a password and the password protected message will appear.

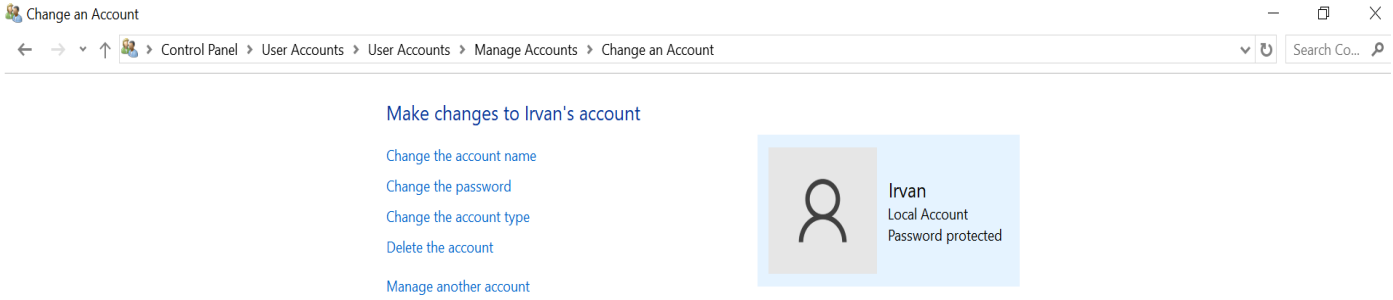


Figure 12. Account is protected

The account has been created and password-protected. Then, press the Windows + L keys on your keyboard, and a locked laptop screen will appear.

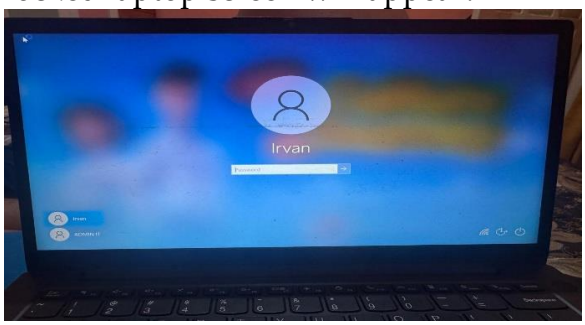


Figure 13. Laptop Lock is Locked

There are 2 accounts in the image, Irvan indicates the user and ADMIN IT as the administrator.

D. Regular inventory data updates and periodic stocktaking activities Regular inventory data updates and periodic stocktaking activities are important activities in asset management, especially information technology assets, to ensure the accuracy, completeness, and reliability of the organization's inventory data. Inventory updates are carried out routinely to reflect the actual condition of assets, including the addition of new assets, the removal of assets that are no longer used, and changes in ownership status, location, or responsibility of assets. With up-to-date inventory data, organizations can manage assets more effectively and minimize the risk of loss, misuse, or uncontrolled use of assets. The following table shows updated IT inventory data.

DATA INVENTARIS IT						
No	Perangkat	No Inventaris	NIPP	PENGGUNA	JABATAN	KETERANGAN
1	Laptop	IT.007.0622.1.C031.00006	62477	SLAMET WAHYUDI	ASSISTANT MANAGER IT 1	UPDATE
2	Laptop	IT.007.0422.1.C031.00002	62176	DECKY AJIARMAN	ASSISTANT MANAGER IT 2	UPDATE
3	Laptop	IT.007.0622.1.C031.00005	61538	SAPRIZAL PRATAMA	ASSISTANT MANAGER IT 3	UPDATE
4	Laptop	IT.007.0523.1.C031.00002	72690	IRVAN RAMADHAN	PELAKSANA IT 1	UPDATE
5	Laptop	IT.007.0422.1.C031.00001	63961	M.FARID RAMADHAN	PELAKSANA IT 2	UPDATE
6	Laptop	IT.007.0523.1.C031.00002	72116	M.AGUNG MAHYUDINATA	PELAKSANA IT 2	UPDATE

Table 14. IT Inventory Data

Meanwhile, periodic stocktaking is conducted as a form of physical verification of inventory data recorded in the system. The purpose of stocktaking is to match administrative data with asset conditions in the field, thus identifying any discrepancies, inconsistencies, or potential problems, such as lost, damaged, or poorly documented assets. The results of stocktaking serve as the basis for correcting inventory data and evaluating the ongoing asset management process.

Figure 15. Inventory Number on Device

E. replacement or refilling of APAR and routine monthly inspections

This activity is a crucial part of safety control and emergency preparedness efforts within the information systems unit. Fire extinguishers (APARs) are replaced or refilled when their expiration date has expired, the safety seal is broken, or the fire extinguisher has been used. This action ensures that the fire extinguisher is always ready for use in the event of a fire emergency.

Figure 16. Replacing the APAR

3. Check Stage (Inspection)

At the Check stage, it is related to Clause 9 of ISO/IEC 27001, in clause 9.1 Internal Audit which regulates the information system unit to carry out periodic internal audits to ensure that the ISMS has been implemented and maintained in accordance with the requirements of ISO/IEC 27001 and the organization's internal provisions.

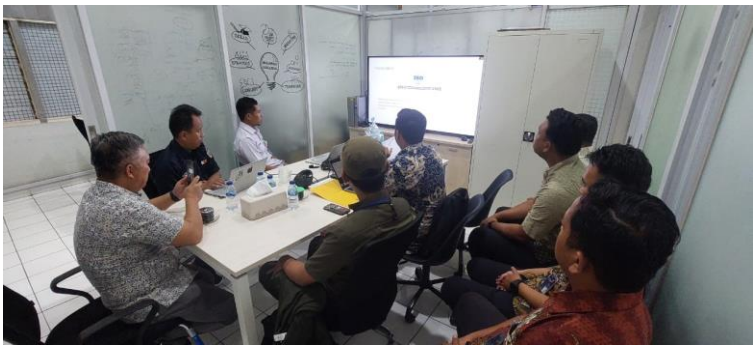


Figure 17. Audit Activities

After the audit was conducted, a description of the discrepancy was found on the form, namely that the device had not been set to the ntp.kai.id time in accordance with the applicable provisions based on ISO Reference A.8.17 Clock synchronization. Evidence of findings on the device with inventory number IT.007.0523.1.C031.00002 with open status.

	PT KERETA API INDONESIA (PERSERO) SISTEM INFORMASI	Nomor	FR.SM/TI/006.003/10-2020
		Tanggal	12 Oktober 2020
	FORMULIR KETIDAKSESUAIAN	Versi	002-2020
		Halaman	4 dari 7

No. Ref	:	___/___/_____
Tanggal	:	23/01/2024
Business Area	:	C031

Tanggal	:	03/12/2025	**Auditor / Pelapor**	:	Raushan Fikri
Nomor Laporan	:	2025-AI-DV3-04	**Auditee**	:	IT DIVRE 3 Palembang
Kriteria	:	ISO/IEC 27001:2022	**Klasifikasi Temuan**	:	Minor

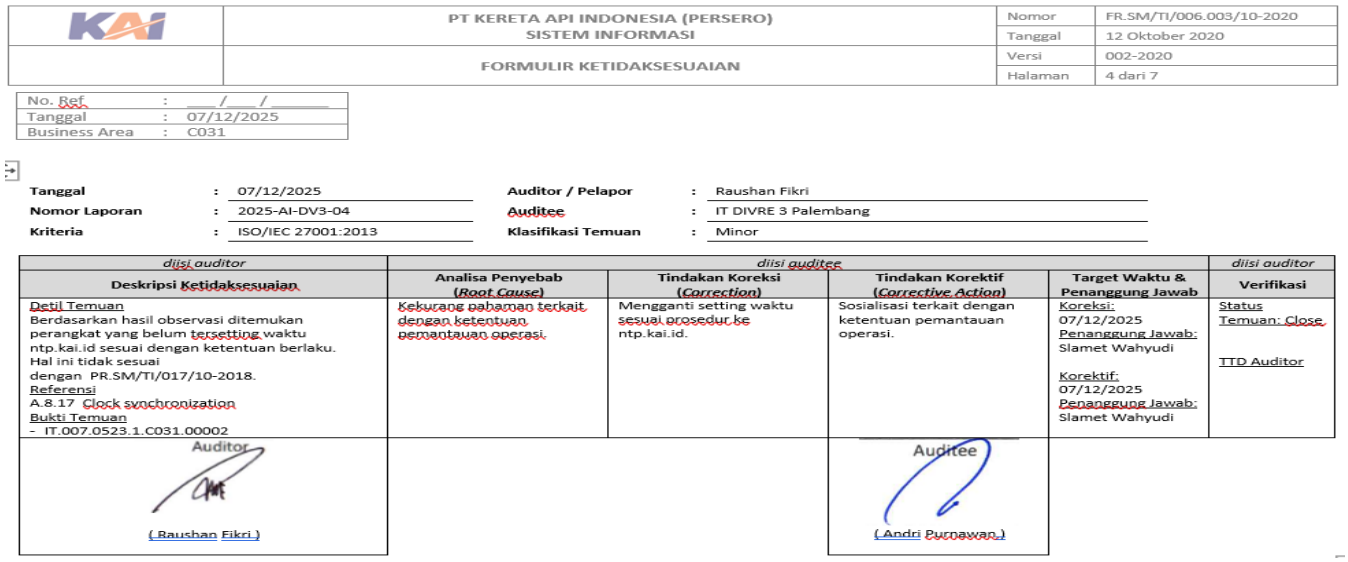
diisi auditor	*diisi auditee*				*diisi auditor*
Deskripsi Ketidaksesuaian	**Analisa Penyebab (*Root Cause*)**	**Tindakan Koreksi (*Correction*)**	**Tindakan Korektif (*Corrective Action*)**	**Target Waktu & Penanggung Jawab**	**Verifikasi**
Detil Temuan Berdasarkan hasil observasi ditemukan perangkat yang belum tersetting waktu ntp.kai.id sesuai dengan ketentuan berlaku. Hal ini tidak sesuai dengan PR.SM/TI/017/10-2018. Referensi A.8.17 Clock synchronization Bukti Temuan - IT.005.0824.6.A010.00307	Kekurangpahaman terkait dengan ketentuan pemantauan operasi.	Mengganti setting waktu sesuai prosedur ke ntp.kai.id.	Sosialisasi terkait dengan ketentuan pemantauan operasi.	Koreksi: 07/12/2025 Penanggung Jawab: Slamet Wahyudi Korektif: 07/12/2025 Penanggung Jawab: Slamet Wahyudi	Status Temuan: Open TTD Auditor
Auditor (Raushan Fikri)			Auditee (Andri Purnawan)		

Figure 18. Open Non-Conformance Form

Based on the findings of the Laptop device with inventory number IT.007.0523.1.C031.00002, it was found that the time setting was not in accordance with procedures and was given a repair period of 4 days with the status being open.

4. Act Stage (Corrective Action)

At the Act stage, related to Clause 10 of ISO/IEC 27001, Clause 10.1 Non-Conformities and Corrective Actions emphasizes that the information system unit is obliged to handle any non-conformities found in the implementation of the Information Security Management System (ISMS). These non-conformities are generally obtained from the results of internal audits in Clause 9.2. The corrective action taken is to change the time setting according to the procedure to ntp.kai.id. With these results, the findings become Closed, as seen in the image below.



	PT KERETA API INDONESIA (PERSERO) SISTEM INFORMASI	Nomor	FR.SM/TI/006.003/10-2020
		Tanggal	12 Oktober 2020
	FORMULIR KETIDAKSESUAIAN	Versi	002-2020
		Halaman	4 dari 7

No. Ref	:	___/___/___
Tanggal	:	07/12/2025
Business Area	:	C031

Tanggal	:	07/12/2025	**Auditor / Pelapor**	:	Raushan Fikri
Nomor Laporan	:	2025-AI-DV3-04	**Auditee**	:	IT DIVRE 3 Palembang
Kriteria	:	ISO/IEC 27001:2013	**Klasifikasi Temuan**	:	Minor

diisi auditor	*diisi auditee*				*diisi auditor*
Deskripsi Ketidaksesuaian	**Analisa Penyebab (*Root Cause*)**	**Tindakan Koreksi (*Correction*)**	**Tindakan Korektif (*Corrective Action*)**	**Target Waktu & Penanggung Jawab**	**Verifikasi**
Detil Temuan Berdasarkan hasil observasi ditemukan perangkat yang belum tersetting waktu ntp.kai.id sesuai dengan ketentuan berlaku. Hal ini tidak sesuai dengan PR.SM/TI/017/10-2018. Referensi A.8.17 Clock synchronization Bukti Temuan - IT.007.0523.1.C031.00002	Kekurang pahaman terkait dengan ketentuan pemantauan operasi.	Mengganti setting waktu sesuai prosedur ke ntp.kai.id.	Sosialisasi terkait dengan ketentuan pemantauan operasi.	Koreksi: 07/12/2025 Penanggung Jawab: Slamet Wahyudi Korektif: 07/12/2025 Penanggung Jawab: Slamet Wahyudi	Status Temuan: Close TTD Auditor
Auditor (Raushan Fikri)			Auditee (Andri Purnawan)		

Figure 19. Close Non-Conformity Form

Based on the findings of the laptop device with inventory number IT.007.0523.1.C031.00002, repairs have been carried out and the auditor has included proof of signature with a statement of open status.

Conclusion

This study found that the Information System Unit of PT KAI Divre III Palembang has effectively implemented ISO/IEC 27001:2013 through the PDCA cycle, with key achievements in the Plan stage such as filling out NDAs, a clear organizational structure, risk assessment using a probability-impact matrix, and socializing security awareness. The Do stage demonstrated practical controls such as antivirus installation, disabling the save password feature, locking devices, updating IT asset inventory, and replacing fire extinguishers, which successfully reduced the risk from high and medium to low. In the Check and Act stages, internal audits identified device time synchronization discrepancies, which were immediately corrected, demonstrating the ongoing commitment to the ISMS. Practical implications include increasing operational resilience in the state-owned transportation sector, preventing downtime and data leaks that impact public services in South Sumatra.

However, the study's limitations lie in its qualitative descriptive approach with a purposive sample of 10 respondents, which limits generalizability to other divisions of PT KAI, and the lack of quantitative measurement of post-implementation security metrics. Suggestions for further research include cross-division comparative studies with quantitative analysis using tools such as the NIST Cybersecurity Framework, evaluation of the long-term effectiveness of Annex A controls, and integration of AI for real-time threat detection to complement this gap analysis.

References

Alreemy, Z., Chang, V., Walters, R., & Wills, G. (2022). Critical success factors of information security management and their impact on information security effectiveness and maturity: A fuzzy TISM approach. Journal of Information Security and Applications, 61, Article 103287. https://doi.org/10.1016/j.jisa.2021.103287

Calder, A., & Watkins, S. (2015). IT governance: An international guide to data security and ISO27001/ISO27002 (6th ed.). Kogan Page.

Creswell, J. W., & Poth, C. N. (2022). Qualitative inquiry and research design: Choosing among five approaches (5th ed.). SAGE Publications.

Damanik, R., Zaki, A., & Fiddarain, M. (2023). Implementation of ISO 27001:2013 in securing information systems at the ANNUR PRIMA Islamic Education Foundation. Information Security Journal, 8(2), 101–110.

Deming, W.E. (1986). Out of the crisis. MIT Press.

Emzir. (2021). Qualitative research methodology: Qualitative data analysis. Student Library.

Fernandez, E. B., Monge, R., & Hashizume, K. (2024). Building a security reference architecture for cloud systems. Requirements Engineering, 29(1), 1–25. https://doi.org/10.1007/s00766-023-00415-2

Goel, S., & Shawky, H. A. (2021). Cybersecurity for transportation systems. Journal of Transportation Security, 14(3-4), 145–167. https://doi.org/10.1007/s12198-021-00234-5

Goetsch, D. L., & Davis, S. B. (2016). Quality management for organizational excellence: Introduction to total quality (8th ed.). Pearson.

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. BSI Publishing.

Intan Mafiana, A., Hanum, L., Ilmi, HM, & Febriliani, S. (2023). Implementation of ISO 27001-based information security management in academic information systems. Journal of Digital Business and Innovation Management, 2(2), 139–163.

ISO/IEC. (2013). ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization.

ISO/IEC. (2022). ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.

Kalaimannan, E., Nguyen, H., & Periga, M. (2021). Password management practices and perceptions. Computers & Security, 105, Article 102241. https://doi.org/10.1016/j.cose.2021.102241

Mesquida, A.-L., Mas, A., & O Connor, R.V. (2021). Integrating cybersecurity in software engineering processes. Journal of Software: Evolution and Process, 33(5), e2325. https://doi.org/10.1002/smr.2325

Nugroho, E., Pratama, R., & Sari, DP (2023). Risk assessment in information security management systems: A case study in Indonesian state-owned enterprises. Journal of Information Technology, 17(1), 20–35.

Peltier, T.R. (2016). Information security policies, procedures, and standards: Guidelines for effective information security management. CRC Press.

Pratama, R., & Nugroho, E. (2018). Evaluation of the level of compliance of information security management systems using ISO/IEC 27001:2013. Journal of Information Technology, 12(1), 45–54.

Rahman, F., & Putra, A. (2017). Designing an information security management system using ISO/IEC 27001:2013. Journal of Computer Science and Information Security, 9(2), 60–68.

Riana, N., Sulistyawati, E., & Putra, A. (2023). Analysis of maturity level and PDCA (plan-do-check-act) in the implementation of information security management system audit at PT Indonesia Game using the ISO 27001:2013 method. Journal of Information Systems and Security, 11(1), 55–64.

Ritzkal, Goeritno, A., & Hendrawan, AH (2019). Implementation of ISO/IEC 27001:2013 for information security management systems (ISMS) at the Faculty of Engineering, UIKA-BOGOR. Information Systems Journal, 15(2), 85–95.

Sari, DP, Winarno, WW, & Hidayat, R. (2020). Analysis of the implementation of an ISO/IEC 27001:2013-based information security management system in academic information systems. Informatics Journal, 14(3), 210–220.

Siponen, M., Vance, A., & Willison, R. (2022). New insights into theorizing information security behavior. MIS Quarterly, 46(1), 1–28. https://doi.org/10.25300/MISQ/2022/16200

Stallings, W. (2017). Effective cybersecurity: A guide to using best practices and standards. Pearson.

Sudaryono. (2022). Educational research methodology. Rineka Cipta.

Sugiyono. (2021). Quantitative, qualitative, and R&D research methods. Alfabeta.

Susanto, H., & Almunawar, MN (2021). Information security management systems: A novel framework and software as a tool for compliance with information security standards. Journal of King Saud University - Computer and Information Sciences, 33(7), 819–831. https://doi.org/10.1016/j.jksuci.2019.04.006

Utami, N., & Kurniawan, Y. (2021). Analysis of the level of readiness for implementing ISO/IEC 27001:2013 in educational organizations. Journal of Informatics Management, 16(1), 33–42.

Whitman, M. E., & Mattord, H. J. (2018). Principles of information security (6th ed.). Cengage Learning.