ISSN: 2338-8412 e-ISSN : 2716-4411

Ekombis Review – Jurnal Ilmiah Ekonomi dan Bisnis
Available online at : https://jurnal.unived.ac.id/index.php/er/index
DOI: https://doi.org/10.37676/ekombis.v14i2

Information Security Management System Transition Strategy From ISO/IEC 27001:2013 To ISO/IEC 27001:2022 At PT PKT

Puguh Prasetyo [1]; Gatot Yudoko [2]
[1,2)]Master of Business Administration Program Institut Teknologi Bandung
Email: [1)]29123489@mahasiswa.itb.ac.id ;[2)] gatot@sbm-itb.ac.id

How to Cite :
Prasetyo, P., Yudoko, G. (2026). Information Security Management System Transition Strategy from ISO/IEC 27001:2013 to ISO/IEC 27001:2022 at PT PKT. EKOMBIS REVIEW: Jurnal Ilmiah Ekonomi Dan Bisnis, 14(2). DOI: https://doi.org/10.37676/ekombis.v14i2

ARTICLE HISTORY
Received [02 December 2025]
Revised [25 April 2026]
Accepted [28 April 2026]

KEYWORDS
Information Security Management Systems, ISO 27001:2022, Transition ISO 27001, Gap Analysis, PDCA Cycle, Network Planning, Critical Path Method.

ABSTRACT

ISO issued the ISO/IEC 27001:2022 standard in October 2022 to update ISO/IEC 27001:2013 with the main objective of improving the relevance of the standard to the current state of information security, ensuring simpler and more effective controls, and facilitating better risk handling. The transition period given is for 3 years since the latest standard was published in October 2022, ISO provides a transition period until October 31, 2025 so that organizations can adjust their information security management systems to the latest version. After that date, ISO/IEC 27001:2013 certification is declared invalid, and all organizations that want to maintain their certification must comply with the latest ISO/IEC 27001:2022 standard.The proposed solution from this research is thirteen action plans to be implemented by PT PKT to close the identified gaps and to meet all the requirements in ISO/IEC 27001:2022. The action plans are grouped according to Plan-Do-Check-Action (PDCA) cycle adopted by ISO as the basis for consideration in preparing the implementation time frame. The results of the research showed that PT PKT could make a transition in eight months. The implementation of proposed action plan starts in July 2024 and will completed in February 2025, which means that PT PKT can successfully transition ISO/IEC 27001:2022 before the due date.

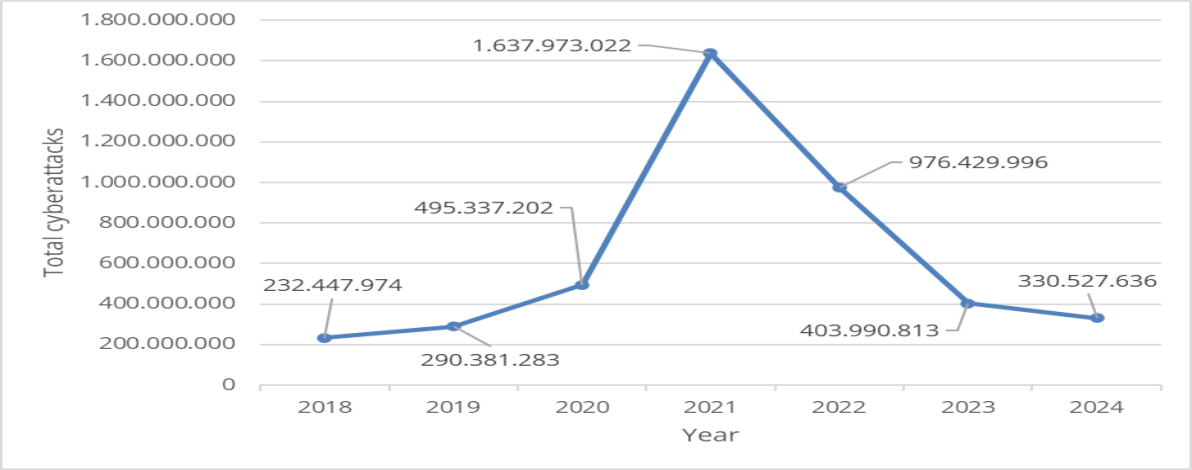
INTRODUCTION

One of Southeast Asia's largest digital economies, Indonesia has demonstrated a strong commitment to bolstering cybersecurity in order to sustain the sustainability of digital transformation. The significance of safeguarding information assets is highlighted by the rise in cyberthreats like ransomware, phishing, and data breaches. The adoption of an ISMS based on ISO/IEC 27001:2022 is a strategic step to boost public trust and maintain business sustainability

in various sectors, as the potential for digital economic growth is predicted to reach USD 146 billion by 2025 (Good News from Indonesia, 2024).

According to the report on cybersecurity monitoring that was published by the National Cyber and Crypto Agency (BSSN), the average total anomalous traffic of cyberattacks in Indonesia has reached more than 600,000 per year over the course of the past seven years. The occurrence of this anomalous traffic activity can have a number of consequences, including a decrease in the performance of devices and networks, the theft of sensitive data, damage to an organization's reputation, and a reduction in trust in the organization (BSSN, 2025).

Figure 1. Cyberattack Anomaly Graph in Indonesia



The Indonesian government issued Presidential Regulation Number 95 of 2018 concerning the Electronic-Based Government System (SPBE) as a follow-up to the strengthening of national information security. The purpose of this regulation is to increase the efficiency and security of information systems in a variety of sectors. According to article 1, SPBE is the implementation of government that makes use of information and communication technology in an integrated manner in order to improve governance. In addition to ensuring the protection of data and information security, the purpose of the SPBE is to guarantee the efficacy, transparency, and accountability of public services. To be more specific, Article 19 stipulates that every government agency is obligated to implement information and communication technology governance, which includes information security risk management, in order to safeguard the confidentiality, integrity, and availability (CIA) of information that is managed (BPK, 2025).

In order to address the growing complexity of challenges arising from both internal and external sources that lead to swift changes in the business landscape, PT PKT must consistently enhance every facet of its operations. PT PKT developed a digital transformation program to address these challenges, focusing on enhancing the Company's efficiency, productivity, and competitiveness. PT PKT established an Industry 4.0 policy in 2018 as part of its digital transformation program. The policy highlights the necessity of integrating automation across all factories and throughout the Company's business processes in alignment with the Information Technology Master Plan. In 2019, PT PKT achieved the Indonesia Industry 4.0 Readiness Index (INDI 4.0) award as part of its digital transformation program, thanks to the implementation of various innovations within the Company, initiated by the Government. Furthermore, in 2021, PT PKT was awarded the National Lighthouse Industry 4.0 designation by the Ministry of Industry for its successful implementation of Industry 4.0-based technology in the Company's operational processes.

The scope of implementation for the implementation and certification of ISO/IEC 27001:2013 is as follows: the management of digital and non-digital information in company operations through an information security management system, covering all supporting devices

for the implementation of the ISMS such as: servers, applications and databases, networks, hardware and software supporting services, procedures and governance, and human resources. PT PKT has obtained the ISMS ISO/IEC 27001:2013 certificate for the first time in 2021, issued by an accredited certification body, the National Accreditation Committee (KAN). The benefits of implementing an ISMS are maintaining the status zero corporate information security incidents. In addition, intangible benefits include increased employee awareness of corporate data and information security issues, fulfilling the cyber security clause in the Baldrige Excellence Framework (BEF) assessment so that the Company gets the Industry Leader predicate and supporting the Environmental, Social, and Governance (ESG) assessment so that PT PKT gets the Medium Risk predicate in the ESG risk rating.

Business Issue

In October 2022, ISO released the ISO/IEC 27001:2022 standard to revise the 2013 version. The primary aim was to enhance the standard's relevance to contemporary information security conditions, streamline controls for greater effectiveness, and improve risk management practices. ISO has established a 3-year transition period following the publication of the latest standard in October 2022, extending until October 31, 2025, allowing organizations to adjust their ISMS to the most recent version. Following that date, ISO/IEC 27001:2013 certification becomes invalid, and all organizations seeking to retain their certification must adhere to the updated ISO/IEC 27001:2022 standard.

Engaging essential stakeholders who provide insights from strategic, operational, and technical viewpoints is vital when addressing the issue of PT PKT's transition of its Information Security Management System (ISMS) from ISO/IEC 27001:2013 to the 2022 version. The board of directors serves as the primary decision-making body, responsible for allocating necessary resources and aligning the ISMS transition with the strategic objectives of the organization. The organization's priorities are evident in the problem definition, backed by strong executive support. The Vice President of Information Technology is one of the problem owners since they oversee the daily operations and documentation of the ISMS and are thus most familiar with its real-world constraints. Furthermore, as the Secretary of the Management Representative, the Vice President of Integrated Management System & Innovation is essential in integrating the ISMS with other systems and guaranteeing audit readiness. These people are crucial in communicating the organization's actual compliance risks and challenges. The ISMS team, on the other hand, consists of problem solvers who possess the technical know-how to evaluate the discrepancy between present and future controls and suggest workable solutions. Furthermore, by pointing out flaws that could prevent a successful certification to the new standard, the internal audit team offers a compliance-driven viewpoint. All of these stakeholders' participation guarantees that the issue is thoroughly understood from all perspectives (strategic, operational, and technical), offering a thorough foundation for an efficient and well-coordinated remediation plan.

LITERATURE REVIEW

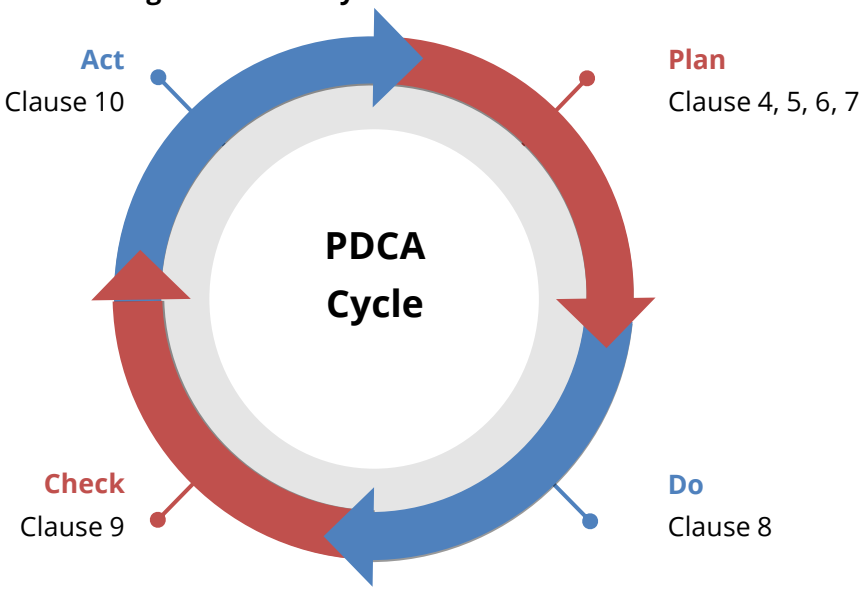
The literature review was conducted to understand current business problems and determine optimal actions in resolving them, by referring to various relevant theories and concepts to verify research problems, show the urgency of problem formulation.

PDCA Cycle in ISO/IEC 27001:2022

The PDCA cycle is a fundamental methodology embedded within ISO/IEC 27001:2022 to ensure systematic and iterative enhancement of information security processes. it is essential to understand the application of the PDCA cycle in ISO/IEC 27001:2022 to recognize its role in the

continuous improvement of an ISMS. The PDCA cycle in ISO/IEC 27001:2022 is illustrated in the following figure:

Figure 2. PDCA Cycle in ISO/IEC 27001:2022



Continual Improvement in ISO/IEC 27001:2022

In the context of ISO/IEC 27001:2022, the term continual improvement is emphasized, particularly in Clause 10.1, which requires organizations to continually improve the suitability, adequacy, and effectiveness of the ISMS. While continuous improvement refers to an ongoing, uninterrupted effort to improve processes, continual improvement implies a more iterative approach, involving periodic assessments and improvements. This distinction is crucial in ISO 27001 as it recognises that improvements may not be constant but should be made on a regular basis to adapt to evolving information security risks. Therefore, ISO/IEC 27001:2022 adopts the concept of continual improvement to ensure that organizations systematically and periodically evaluate and improve their ISMS in line with the dynamic nature of information security threats (IT Governance USA, 2024).

Network Planning with Critical Path

Network planning is one of the management approaches that can help in planning and controlling a project. A project schedule network diagram is a graphical representation of the logical relationships between project schedule activities, often known as dependencies. Network planning uses two basic techniques: the Critical Path Method (CPM) and the Program Evaluation Review and Technique (PERT). CPM is a time-oriented technique that produces deterministic estimates of time and cost. PERT is a time-oriented strategy that produces probabilistic schedules and times (Mar'aini and Rahmat Akbar, 2022). In this study, the author uses network planning with critical path to determine the optimal project completion time by identifying activities that do not have time slack so that timely decisions and better risk management are obtained during project implementation.

METHODS

The research design is starting by identifying business issue, research question and research objective, literature review, data collection, data analysis to determine business solutions, implementation plan and results.

The first step taken by the researcher is to identify the problem that exists by identifying the issue faced by PT PKT. Identification is done by interviewing the Integrated Management

System and Innovation Vice Precident, Information Technology Vice Precident and reviewing news on the ISO website related ISMS development. The following step are a research question and research objectives. The author defines the research question and sets goals to provide focus and direction for this research and to help avoid any distraction from the topic. The next step is literature review. A literature review is used to review all the literature that helps in solving the problems. The author examines the ISO/IEC 27001:2013 and ISO/IEC 27001:2022 standards, as well as a review of the approach used in ISO/IEC 27001 and the method of gap analysis. After the literature review, the next step is data collection for the research.

The data collection used by the author in this study is divided into two categories, namely primary and secondary data.

a. Primary data

Primary data is collected through a discussion process with the Vice President of Information Technology as the person in charge of ISMS intensively. In addition, the primary data collection process also involves the ISMS secretary and the Vice President of Integrated Management System & Innovation as the Management Representative to identify obstacles that arise during the implementation of ISMS. The following is a list of interview questions for the sources.

Table 1. List of Interview Questions for Source Persons

No	Source Person	Topic	Interview Questions	References
1	Vice President of Information Technology	General Understanding and Motivation	What are the primary motivations for transitioning to ISO 27001?	Shojaie B., Federrath H., Saberi I. (2016); Mera-Amores F., Roa H.N. (2024)
			How familiar are you with the core objectives and benefits of ISO 27001?	Mera-Amores F., Roa H.N. (2024)
		Implementation Challenges	What are the main challenges you foresee in terms of time, effort, and cost for the transition?	Shojaie B., Federrath H., Saberi I. (2016)
			What cultural barriers do you anticipate in implementing ISO 27001, and how do you plan to address them?	Mera-Amores F., Roa H.N. (2024)
		Risk Management and Continuous Improvement	How do you plan to integrate risk management into your ISO 27001 implementation?	Evang J.M. (2022); Fletcher W.J. (2015)
			What measures will you put in place to ensure continuous improvement post-certification?	Healy J. (2003); Farmer N. (2003)

2	VP of Integrated Management System & Innovation	Resource and Role Management	How do you plan to allocate resources and roles for the ISO 27001 implementation?	Mera-Amores F., Roa H.N. (2024)
			What strategies will you use to ensure cooperation and compliance from all employees?	Khurshid A., Imran S. (2011)
		Compliance and Integration	How will you ensure compliance with other relevant regulations and standards during the transition?	Lopes I.M., Guarda T., Oliveira P. (2019)
			What is your plan for integrating ISO 27001 with existing management systems?	Healy J. (2003); Ţigănoaia B. (2015)
3	ISMS Secretary	Process and Documentation	What steps will you take to ensure that all necessary documentation is complete and accurate?	Khurshid A., Imran S. (2011)
			How will you conduct internal audits to prepare for the final external audit?	Khurshid A., Imran S. (2011)
		Stakeholder Engagement	How will you communicate the business value of ISO 27001 certification to stakeholders?	Khurshid A., Imran S. (2011).
			What role will top management play in the transition process?	Farmer N. (2003)

b. Secondary data
Secondary data is collected from the PT PKT website, ISO/IEC 27001 Standards versions 2013 and 2022, journals and articles from official websites on the internet.

RESULTS

This chapter presents the results of the analysis obtained from primary and secondary data related to the readiness of the ISMS transition from ISO/IEC 27001:2013 to ISO/IEC 27001:2022 at PT PKT. This analysis focuses on identifying the gap between the current implementation conditions and the requirements of the latest standard, as well as determining the action plan and challenges that may be faced and the support needed during the transition process.

Comparison of Requirements for ISO/IEC 27001:2013 and 2022 version

In the ISO/IEC 27001:2022 standard, there are several changes such as the addition of new Clauses and new Sub-Clauses. ISO/IEC 27001:2013 has adopted the High-Level Structure (HLS) and in the 2022 version it is still maintained, this is intended so that this standard can be integrated with other ISO standards that also adopt HLS. The differences in the Clause structure of ISO/IEC 27001:2013 and ISO/IEC 27001:2022 are illustrated in the following figure:

Figure 3. Comparison of ISO/IEC 27001:2013 and 2022 Structure

ISO/IEC 27001:2013		ISO/IEC 27001:2022
1. Scope	→	1. Scope
2. Normative references	→	2. Normative references
3. Terms and definitions	→	3. Terms and definitions
4. Context of the organization	→	4. Context of the organization
4.1. Understanding the organization and its context	→	4.1. Understanding the organization and its context
4.2. Understanding the needs and expectations of interested parties	→	4.2. Understanding the needs and expectations of interested parties
4.3. Determining the scope of the information security management system	→	4.3. Determining the scope of the information security management system
4.4. Information security management system	→	4.4. Information security management system
5. Leadership	→	5. Leadership
5.1. Leadership and commitment	→	5.1. Leadership and commitment
5.2. Policy	→	5.2. Policy
5.3. Organizational roles, responsibilities and authorities	→	5.3. Organizational roles, responsibilities and authorities
6. Planning	→	6. Planning
6.1. Actions to address risks and opportunities	→	6.1. Actions to address risks and opportunities
6.1.1. General	→	6.1.1. General
6.1.2. Information security risk assessment	→	6.1.2. Information security risk assessment
6.1.3. Information security risk treatment	→	6.1.3. Information security risk treatment
6.2. Information security objectives and planning to achieve them	→	6.2. Information security objectives and planning to achieve them
-	→	6.3. Planning of changes
7. Support	→	7. Support
7.1. Resources	→	7.1. Resources
7.2. Competence	→	7.2. Competence

7.3. Awareness	7.3. Awareness
7.4. Communication	7.4. Communication
7.5. Documented information	7.5. Documented information
7.5.1. General	7.5.1. General
7.5.2. Creating and updating	7.5.2. Creating and updating
7.5.3. Control of documented information	7.5.3. Control of documented information
8. Operation	8. Operation
8.1. Operational planning and control	8.1. Operational planning and control
8.2. Information security risk assessment	8.2. Information security risk assessment
8.3. Information security risk treatment	8.3. Information security risk treatment
9. Performance evaluation	9. Performance evaluation
9.1. Monitoring, measurement, analysis and evaluation	9.1. Monitoring, measurement, analysis and evaluation
9.2. Internal audit	9.2. Internal audit
	9.2.1. General
	9.2.2. Internal audit programme
9.3. Management review	9.3. Management review
	9.3.1. General
	9.3.2. Management review inputs
	9.3.3. Management review results
10. Improvement	10. Improvement
10.1. Nonconformity and corrective action	10.1. Continual improvement
10.2. Continual improvement	10.2. Nonconformity and corrective action
Annex A. Reference control objectives and controls (114 controls & 14 categories)	Annex A. Information security controls reference (93 controls & 4 categories)

Based on information from the table, the ISO/IEC 27001 standard versions 2013 and 2022 still use HLS which consists of 10 Clauses, but there are additional Clauses and several Sub-Clauses in the 2022 version, including: the addition of Clause 6.3, the addition of Sub-Clauses 9.2.1, 9.2.2, 9.3.1, 9.3.2, 9.3.3 and changes to the Annex, where in the 2013 version there were 114 controls and 14 categories, while in the 2022 version there are 14 controls and 4 categories (ANSI, 2023).

List of Action Plan

The action plan that must be carried out to close the results of the gap analysis between the current system and ISO/IEC 27001:2022 will be summarized in Table 2 as follows:

Table 2. Set of Action Plans for ISO/IEC 27001:2022 Transition

No	Action Plan
1	Update the list of internal and external issues, Statement of Applicability (SOA) and *Pedoman Sistem Manajemen Keamanan Informasi* document
2	Update the ISMS risk identification list
3	Identify and creat work instructions for new controls
4	Conduct awareness training for all employees
5	Conduct internal audit training for ISMS internal auditors
6	Conduct ISMS internal audit
7	Follow up on internal audit findings
8	Conduct management review
9	Follow up on management review meeting result
10	Conduct external audit stage 1
11	Follow up on external audit stage 1
12	Conduct external audit stage 2
13	Follow up on external audit stage 2

All of these action plans will be prioritized using the PDCA cycle. The PDCA cycle is used as the basis for prioritization because the ISO/IEC 27001 standard employs this method in both the 2013 and 2022 versions. To accelerate the transition process specifically, the action plan related to the implementation of awareness training for all employees and internal audit training for the ISMS auditor team in the "Do" step will be carried out first.

Table 3. ISO/IEC 27001:2022 Transition Action Plan Sequence at PT PKT

Step	Action Plan	PDCA
1	Conduct awareness training for all employees	Do
2	Conduct internal audit training for ISMS internal auditors	Do
3	Update the list of internal and external issues, Statement of Applicability (SOA) and Pedoman Sistem Manajemen Keamanan Informasi document	Plan
4	Update the ISMS risk identification list	Plan
5	Identify and creat work instructions for new controls	Plan
6	Conduct ISMS internal audit	Check
7	Follow up on internal audit findings	Action
8	Conduct management review	Check
9	Follow up on management review meeting result	Action
10	Conduct external audit stage 1	Check
11	Follow up on external audit stage 1	Action
12	Conduct external audit stage 2	Check
13	Follow up on external audit stage 2	Action

Implementation Plan & Justification

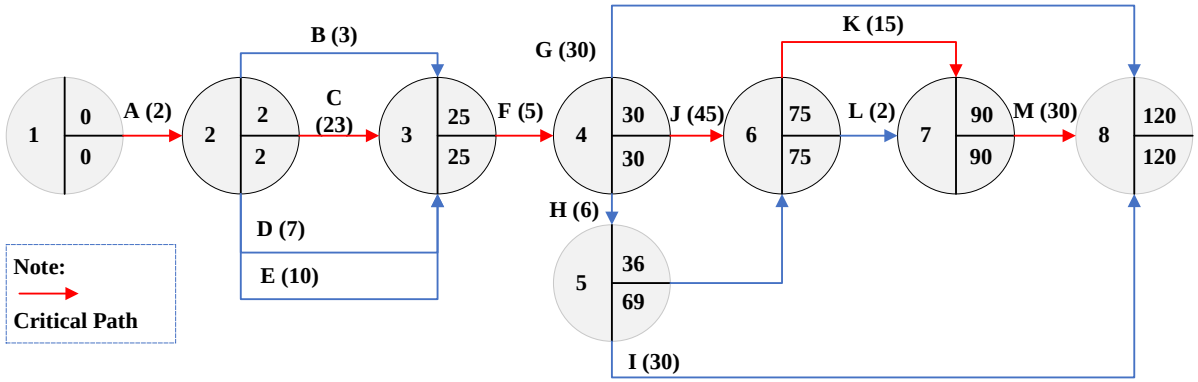
The implementation plan and justification ensure that all action plans can be carried out and that the PT PKT ISO/IEC 27001:2022 transition is completed before the due date. The following table presents details of activities, time estimates, and predecessor activities:

Table 4. Project Activities List

Activities	Action Plan	Predecessor Activities	Duration (Days)
A	Conduct awareness training for all employees	-	2
B	Conduct internal audit training for ISMS internal auditors	A	3
C	Update the list of internal and external issues, Statement of Applicability (SOA) and Pedoman Sistem Manajemen Keamanan Informasi document	A	23
D	Update the ISMS risk identification list	A	7
E	Identify and creat work instructions for new controls	A	10
F	Conduct ISMS internal audit	B, C	5
G	Follow up on internal audit findings	F	30
H	Conduct management review	F	6
I	Follow up on management review meeting result	H	30
J	Conduct external audit stage 1	F, H	45
K	Follow up on external audit stage 1	J	15
L	Conduct external audit stage 2	J, K	2
M	Follow up on external audit stage 2	L	30

The implementation plan was prepared using network planning and critical path methods as follows:

Figure 4. Critical Path Method in Transition to ISO/IEC 27001:2022



The total time needed for the transition to ISO/IEC 27001:2022 is 120 days, as shown in the Figure 4. PT PKT should pay particular attention to the critical path: steps A, C, F, J, K, and M. Specifically, steps C, J, K, and M, as they require significant time and support from the ISMS team and top management.

The initial stage of the transition begins with building the capacity of employees and the ISMS team, then continues with training for internal auditors who will be assigned to carry out ISMS internal audits. Furthermore, all documents are updated based on the results of the gap analysis. In the next stage, an internal audit, management review is carried out and ends with the implementation of an external audit by a certification body as an accredited external institution, the certification body will issue the ISMS certificate for PT PKT.

DISCUSSION

The lessons learned are used to map the knowledge gained during the ISMS transition implementation based on the PMBOK framework. This knowledge can be managed as an important asset to support PT PKT's implementation of future projects. The following is a list of lessons learned during the implementation of the ISO/IEC 27001:2022 transition at PT PKT:

Table 5. List of Lessons Learned of ISO/IEC 27001:2022 Transition

Category	Lesson Learned	Detail Impact
Schedule Management	Identifying critical activities by using Critical Path Method (CPM) in the transition process is key.	The team was able to target time-sensitive tasks by using CPM to determine the longest path of interdependent activities (such as gap analysis, internal audit, and certification audit). This approach led to a reduction in the probability of project delays and ensured the on-time delivery of critical components. For instance, if "(J) External Audit Stage 1" had not been explicitly marked as critical, resource conflicts with other business priorities would have occurred.
Stakeholder Engagement	Support from Top Management and the ISMS team is essential throughtout the transition.	The involvement of VP Technology Information as the designated reviewer and approver of ISMS guidelines and all requisite work instructions accelerates the ratification process for these documents. This underscores the significance of active engagement and collective ownership among all constituents at PT PKT in implementing ISMS.
Resource Planning	Good activity planning ensures a smooth transition process.	The team was able to target time-sensitive tasks by using CPM to determine the longest path of interdependent activities (such as gap analysis, internal audit, and certification audit). This approach led to a reduction in the probability of project delays and ensured the on-time delivery of critical components. For instance, if "(J) External Audit Stage 1" had not been explicitly marked as critical, it would have been superseded by competing business priorities, resulting in resource conflicts.
Change Management	The transition to ISO/IEC 27001:2022 requires technical adjustments and a change in corporate mindset and behaviour	It is reasonable to hypothesize that employees will encounter challenges when first adapting to stricter information security practices. These practices may include the regulation of USB usage, rules for using external clouds, and other information security protocols. This further underscores the necessity for alterations in both the behaviors of employees and the prevailing culture of the company in order to successfully execute the ISMS transition process.
Knowledge Transfer	It is important to provide teams and employees with competency through	The implementation of regular training and socialization for all employees and the ISMS Team has been shown to increase understanding of how

	awareness training and internal audits in order to build their knowledge and awareness of implementing an ISMS at PT PKT.	to implement ISO/IEC 27001:2022 controls effectively. The number of findings in internal and external audits is minimal, ensuring the smooth execution of the certification process and the timely issuance of ISMS certificates.

CONCLUSION

The author conducted a gap analysis in the transition process from ISO/IEC 27001:2013 to ISO/IEC 27001:2022 at PT PKT. In addition, the author also identified and developed a series of structured action plans to ensure the transition process runs smoothly according to plan and the certificate is issued on time.

1. PT PKT has implemented ISMS and has been certified to ISO/IEC 27001:2013. Currently, PT PKT is transitioning to ISO/IEC 27001:2022 with a due date of October 31, 2025. There is a significant gap in the ISO/IEC 27001 standard version 2013 with 2022, including the development of internal audit clauses and management reviews by adding new sub-clauses and changes in the structure of security controls in Annex A, from 114 controls and 14 categories to 93 controls and 4 categories in the 2022 version. These changes require mapping and determining security controls in the Statement of Applicability (SOA).
2. Based on the gap analysis results, PT PKT requires various improvements to meet the ISO/IEC 27001:2022 standard and enhance overall information security governance, such as preparing employee knowledge and awareness of the new information security standard, preparing the competency of the internal auditor team, evaluating internal and external issues, adjusting management system documents and adjusting information security risks based on the requirements of the new security clauses and controls. These enhancements are imperative not solely for the purpose of adhering to regulatory mandates but also to nurture a more robust and security-conscious corporate culture in the future.
3. The transition process is developed with project management principles based on the PMBOK framework to ensure that the transition is completed before due date. There are 13 action plans identified using the 5W+1H technique, then determined using the PDCA cycle and sorted based on the critical path method (CPM). From the results of the analysis using network planning and CPM, the project duration is estimated to be 120 days, where the activity starts in July 2024 and it is estimated to be completed in February 2025. The estimated duration was obtained using expert and analog assessment methods to support the determination of a realistic schedule.

As outlined in the above description, it can be concluded that a smooth transition process not only considers technical factors but requires a good approach and planning and support from Top Management and the ISMS Team. The results of this study mark a significant milestone for PT PKT to be applied in other companies that will implement ISMS or transition from the ISO/IEC 27001:2013 standard to the latest version.

RECOMMENDATION

Based on the conclusion, the following are recommendations proposed by the author to ensure the success of the ISO/IEC 27001:2022 transition at PT PKT and ensure the implementation of ISMS that is increasingly better and sustainable:

1. Strengthening the position of the ISMS Team by involving departments that are closely related to the implementation of ISO/IEC 27001:2022, namely the Information Technology Department, Corporate Administration Department, Integrated Management System and

Innovation Department, Corporate Risk Management Department and Human Resource Management and Development Department.

2. Integrating change management that includes information security awareness campaigns for all employees, strengthening role models from Top Management and building a corporate culture that has awareness and concern for corporate information security with the aim that corporate information security is the responsibility of all parties in the company, not just the responsibility of the Information Technology Department.
3. The use of the PMBOK framework as a standard for planning project implementation and transition of the entire company management system, this is based on the reasons for the success of using the critical path method and the estimated total duration required in the ISO/IEC 27001:2022 transition process.
4. Maintain a list of lessons learned in the ISO/IEC 27001:2022 transition process as company documentation for continuous improvement, especially in the field of information security. The document will help PT PKT in replicating success in the ISMS implementation cycle in the future and preventing repeated mistakes.
5. Integrate the implementation of ISO/IEC 27001:2022 into the company's Integrated Management System, so that its management is more effective and efficient. Currently there are 4 management systems that have been integrated, namely the Quality Management System ISO 9001:2015, the Environmental Management System ISO 14001:2015, the Occupational Safety and Health Management System ISO 45001:2018 and the Energy Management System ISO 50001:2018.

LIMITATION

This final project is limited to the transition of the ISMS ISO/IEC 27001 according to the scope that has been implemented by PT PKT previously without an integration plan into other Management Systems that have been implemented by PT PKT.

REFERENCES

ANSI (2023). ISO/IEC 27001:2013 & ISO/IEC 27001:2022 Comparison. https://blog.ansi.org/anab/iso-iec-27001-2013-2022-comparison/ (Accessed: 14 April 2025)

BPK (2018). Sistem Pemerintahan Berbasis Elektronik (2025), https://peraturan.bpk.go.id/Details/96913/perpres-no-95-tahun-2018 (Accessed: 23 January 2025)

Cybersecurity Monitoring Report (2025), https://www.bssn.go.id/monitoring-keamanan-siber/ (Accessed: 24 January 2025)

Evang J.M. (2022). ISO 27001 as a Tool for Availability Management. Proceedings - 2022 2nd International Conference on Advanced Enterprise Information System, AEIS 2022, pp. 82-85.

Farmer N. (2003). To deadline and beyond. Quality World, 29 (12), pp. 10 - 12.

Fletcher W.J. (2015). Review and refinement of an existing qualitative risk assessment method for application within an ecosystem-based management framework. ICES Journal of Marine Science, 72 (3), pp. 1043 - 1056.

Good News From Indonesia (2024). Negara dengan Ekonomi Digital Terbesar di Asia Tenggara, Indonesia Urutan ke Berapa? (2025), https://www.goodnewsfromindonesia.id/2024/11/24/negara-dengan-ekonomi-digital-terbesar-di-asia-tenggara-indonesia-urutan-ke-berapa (Accessed: 23 January 2025)

Healy J. (2003). Implementing ISO 9001:2000 - US survey of transition experiences - Statistical analysis. ASQ Annual Quality Congress Proceedings, pp. 297 - 303.

IT Governance USA. (2024). ISO 27001: How to Continually Improve Your ISMS. https://www.itgovernanceusa.com/blog/continual-improvement-and-iso270012013 (Accessed: 14 February 2025)

Khurshid A., Imran S. (2011). The challenge of change at teradata global consulting center (GCC) Pakistan (A and B). Asian Journal of Management Cases, 8 (2), pp. 143-170.

Lopes I.M., Guarda T., Oliveira P. (2019). How ISO 27001 Can Help Achieve GDPR Compliance. Iberian Conference on Information Systems and Technologies, CISTI, 2019-June, art. no. 8760937.

Lopes I.M., Guarda T., Oliveira P. (2019). Implementation of ISO 27001 Standards as GDPR Compliance Facilitator. Journal of Information Systems Engineering and Management, 4 (2), art. no. em0089.

Mar'aini and Rahmat Akbar (2022). Penentuan Jalur Kritis untuk Manajemen Proyek (Studi Kasus Pembangunan Jalan Selensen- Kota Baru- Bagan Jaya). Jurnal Pusat Akses Kajian Manajemen, pp. 13.

Mera-Amores F., Roa H.N. (2024). Enhancing Information Security Management in Small and Medium Enterprises (SMEs) Through ISO 27001 Compliance. Lecture Notes in Networks and Systems, 920 LNNS, pp. 197 - 207.

Shojaie B., Federrath H., Saberi I. (2016). Getting the Full Benefits of the ISO 27001 to Develop an ISMS based on organisations' infosec culture. Proceedings of the 10th International Symposium on Human Aspects of Information Security and Assurance. pp. 88 - 100.

Ţigănoaia B. (2015). Some aspects regarding the information security management system within organizations - Adopting the ISO/IEC 27001:2013 standard. Studies in Informatics and Control, 24 (2), pp. 201 - 210.