Eduvest – Journal of Universal Studies
Volume 6 Number 8, August, 2026
p- ISSN 2775-3735- e-ISSN 2775-3727

Information Security Risk Management in Contactless Toll System Using ISO 27005

Dekaton Punjulhafiidhi*, Rizal Fathoni Aji
Universitas Indonesia, Indonesia
Email: dekaton.0511@gmail.com*, rizal@cs.ui.ac.id

Keywords
Information Security Risk Management; ISO/IEC 27005; Toll Transaction System; Payment System

Abstract
The rapid digital transformation of transportation systems has encouraged the adoption of contactless toll transactions to improve traffic efficiency and user convenience. However, their dependence on real-time processing, continuous availability, sensitive data, and external payment integration creates significant information security risks. This study aims to design an information security risk management framework for the Let It Flo contactless toll transaction system at PT Jasamarga Tollroad Operator using ISO/IEC 27005:2022. A qualitative case study approach was employed, with data collected through semi-structured interviews, direct observations, and organizational documentation. The data were analyzed using thematic analysis, while ISO/IEC 27001:2022 and ISO/IEC 27002:2022 supported the formulation of appropriate security controls. The findings identified 26 information security risk scenarios: three were classified as high risk, twelve as moderate-to-high, two as moderate, and nine as low-to-moderate. Seventeen scenarios required mitigation, whereas nine were considered acceptable under the organization's risk acceptance criteria. Recommended treatments include role-based access control, backup and disaster recovery mechanisms, encryption, penetration testing, physical security controls, system testing, and network redundancy. The study concludes that the ISO/IEC 27005:2022-based framework provides a structured approach to identifying, evaluating, treating, and accepting information security risks, thereby supporting the reliability, security, and continuity of contactless toll transaction services.

INTRODUCTION

The rapid advancement of information technology has accelerated digital transformation across various sectors, including transportation systems (Dimian et al., 2024; Fatorachian et al., 2025; Huang et al., 2023; Li et al., 2023; Nazari & Musilek, 2023; Verma et al., 2024). One of the key innovations is the implementation of contactless toll transaction systems, which enable vehicles to pass through toll gates without stopping by utilizing technologies such as Radio Frequency Identification (RFID) and Automatic Number Plate Recognition (ANPR). These systems operate in real time and significantly improve traffic flow efficiency and user experience (Alsaleh, 2025; Burger & Guna, 2024; Islam, 2025). However, the reliance on continuous system availability and the processing of sensitive user and transaction data

introduce critical challenges related to information security, making such systems highly vulnerable to disruptions and cyber risks.

PT Jasamarga Tollroad Operator (JMTO), as a major toll road operator, has implemented a contactless toll transaction system known as Let It Flo as part of its digital transformation strategy. The system is designed to enhance operational efficiency and reduce congestion at toll gates (Islam, 2025; Muralidharan, 2025). Despite its benefits, several information security incidents have occurred, including system downtime caused by misconfiguration, integration failures with external payment systems, and network connectivity disruptions. These incidents highlight the potential risks associated with system reliability, data integrity, and service availability, which may ultimately affect organizational performance, regulatory compliance, and user trust.

The implementation of information security controls should be supported by a structured management framework to ensure their effectiveness (Grigaliūnas et al., 2024; Herath et al., 2023; Kure et al., 2022; Safitra et al., 2023; Taherdoost, 2022). ISO/IEC 27001:2022 provides the requirements for establishing an Information Security Management System (ISMS), whereas ISO/IEC 27005:2022 offers detailed guidance on information security risk management activities. The integration of these standards enables organizations to adopt a risk-based approach in protecting information assets and maintaining service reliability (International Organization for Standardization, 2022)(International Standard Organization, 2022a). Although ISO/IEC 27005 has been widely implemented in various sectors, most studies focus on conventional information systems such as academic, healthcare, and enterprise environments. Limited research has specifically addressed information security risk management within contactless toll transaction systems that require real-time processing, high availability, and integration with external payment services(Mujib, 2021)(Irfan et al., 2025)(Hidayatullah et al., 2024). Ayo et al. conducted a comprehensive information security risk assessment through asset identification, risk analysis, and risk treatment planning, demonstrating the importance of structured risk management in protecting organizational information assets (Ayo et al., 2018). Previous studies have extensively discussed RFID security and privacy issues, particularly threats related to unauthorized access, eavesdropping, and information leakage (Sharma & P.C, 2013).

However, despite the extensive application of information security risk management in different fields, there is limited research that specifically addresses its implementation in real-time, large-scale contactless toll transaction systems. Existing studies generally focus on conventional information systems and do not fully consider the unique characteristics of transportation systems that require high availability, real-time processing, and integration with multiple external entities. In addition, in the context of JMTO, information security risk management for the Let It Flo system has not yet been formally implemented in a structured and comprehensive manner, which indicates a significant practical gap.

This gap emphasizes the need for a context-specific and systematic risk management framework tailored to critical digital infrastructure systems. Without a structured implementation of information security risk management, organizations may rely on reactive approaches that are insufficient to address emerging and complex security threats. Therefore, it is essential to develop a comprehensive framework that can support proactive risk identification, evaluation, and mitigation, ensuring system reliability and data security.

Based on this context, the objective of this study is to design an information security risk management framework for a contactless toll transaction system using ISO/IEC 27005:2022. This study adopts a qualitative case study approach, utilizing data collected through interviews, observations, and analysis of internal organizational documents. The framework covers key stages, including context establishment, risk assessment, risk treatment, and risk acceptance.

The contribution of this study lies in providing a practical and structured design of information security risk management tailored to a real-world contactless toll transaction system. The results include the identification of risk scenarios, classification of risk levels, and recommendations for mitigation strategies based on international standards. This research is expected to serve as a reference for organizations managing similar critical systems, particularly in the transportation sector, in implementing more effective and systematic information security risk management practices.

METHOD

This study was conducted at PT Jasamarga Tollroad Operator (JMTO) with the research object focused on the Let It Flo system, which is utilized to support Single Lane Free Flow (SLFF) toll transactions. The study aims to develop an information security risk management design for the Let It Flo system as part of organizational efforts to improve information security, system reliability, and service continuity within digital toll transaction operations. The research employed a qualitative approach using a case study method. This approach was selected because the study focuses on an in-depth analysis of information security risk management implementation within a specific organizational environment, namely the Let It Flo system at PT Jasamarga Tollroad Operator. The framework adopted in this study refers to ISO/IEC 27005:2022 as the primary guideline for establishing information security risk management processes, including context establishment, risk assessment, risk treatment, and risk acceptance. Furthermore, ISO/IEC 27001:2022 and ISO/IEC 27002:2022 were used as references in determining information security control recommendations during the risk treatment stage(International Standard Organization, 2022a)(International Standard Organization, 2022b).

Research Design

This study employed a qualitative approach using a case study method to analyze the implementation of information security risk management within the Let It Flo system at PT Jasamarga Tollroad Operator. The qualitative approach was selected because the study focuses on obtaining an in-depth understanding of organizational conditions, operational processes, and information security practices related to the implementation of the system.

The case study method enables researchers to conduct a comprehensive analysis of risk management activities within a specific organizational environment. Through this approach, the study was able to identify existing information security risks, evaluate current controls, and propose risk treatment recommendations based on ISO/IEC 27005:2022 and ISO/IEC 27002:2022 (International Organization for Standardization, 2022)(International Standard Organization, 2022b).

Research Stages

The research stages were conducted systematically to ensure that the entire research process aligned with the objectives of the study. The process began with preliminary data

collection through internal document analysis, direct observation, and interviews with stakeholders involved in the operation and management of the Let It Flo system at PT Jasamarga Tollroad Operator.

Following the preliminary data collection stage, the study continued with problem identification and literature review activities. The collected data were then analyzed using thematic analysis to support the stages of context establishment, risk assessment, risk treatment, and risk acceptance according to ISO/IEC 27005:2022.

Data Collection Methods

Data collection in this study was conducted through interviews, observations, and documentation studies. These methods were selected to obtain comprehensive information regarding operational activities, information security controls, and organizational risk management practices related to the Let It Flo system.

The use of multiple data collection methods was intended to improve the validity and reliability of the research findings. Information obtained from interviews was validated through direct observations and supporting organizational documents.

1. Interview

Interviews were conducted in a semi-structured manner with stakeholders directly involved in information technology management, information security implementation, and system operations at PT Jasamarga Tollroad Operator. The semi-structured approach provided flexibility during the interview process while ensuring that all research objectives were addressed.

The interview process aimed to collect information regarding business processes, security controls, incident handling, operational constraints, and organizational policies related to the Let It Flo system. The informants included personnel from IT Planning and Governance, IT Operations, IT Development, and IT Security divisions.

2. Observation

Observation activities were carried out by directly examining operational processes and information technology activities within the organization. This process enabled researchers to gain a clearer understanding of the actual implementation of information security controls and operational procedures.

The observation process also supported the validation of information obtained from interviews and documentation studies. Through direct observation, the researchers were able to identify actual operational conditions related to system usage, asset management, and information security practices.

3. Documentation Study

The documentation study was conducted by collecting and reviewing organizational documents relevant to the research topic. These documents included internal policies, operational procedures, security guidelines, incident reports, and supporting documents associated with information security management.

The documentation study provided supporting evidence for the research findings obtained from interviews and observations. In addition, the collected documents were utilized to identify existing controls, organizational policies, and risk management practices implemented within the Let It Flo environment.

Data Analysis Method

The data analysis method used in this study was thematic analysis. This method was selected because it allows researchers to identify patterns, themes, and relationships among data obtained from interviews, observations, and documentation studies.

The analysis process began with data transcription and coding activities to classify information into specific themes related to information security risk management. The analysis results were subsequently used as the basis for conducting context establishment, risk identification, risk analysis, risk evaluation, risk treatment, and risk acceptance processes.

Research Instrument

The research instrument used in this study consisted of interview guidelines designed according to the research objectives and data requirements related to information security risk management. The interview questions covered aspects such as information asset identification, threat identification, system vulnerabilities, and existing security controls.

The interview guidelines were designed using a semi-structured format to provide flexibility during the interview process. This approach enabled researchers to explore additional information relevant to the research topic based on the organizational context and responses provided by the informants.

RESULTS AND DISCUSSIONS

Risk Assessment Stage

The risk assessment stage was conducted to identify, analyze, and evaluate risks associated with the Let It Flo non-stop toll transaction system. This process aims to determine potential threats and vulnerabilities that may affect the confidentiality, integrity, and availability of the identified assets. The assessment was performed by analyzing the likelihood and impact of each risk scenario, enabling the determination of risk levels and the prioritization of appropriate risk treatment actions

To evaluate the identified risks, risk criteria were established based on likelihood and impact levels. The likelihood level represents the probability of a risk event occurring, while the impact level reflects the severity of its consequences on the organization's operations, information assets, and services. The combination of these two cristeria is used to determine the overall risk level through the risk matrix shown in Figure 1.

Figure 1. Risk Matrix

To support the risk treatment process, a risk treatment options matrix was established based on the evaluated risk levels. The matrix provides guidance for selecting appropriate treatment strategies according to the severity of each identified risk. As shown in Figure 2, risks

with higher severity levels require mitigation or avoidance actions, while lower-level risks may be accepted and monitored in accordance with the organization's risk acceptance criteria.

Table 1 Risk Treatment Decision Matrix

Risk Level	Risk Treatment Options
Low	Accept/Monitor
Low to Moderate	Reduce/Mitigate or Accept/Monitor
Moderate	Reduce/Mitigate
Moderate to High	Reduce/Mitigate or Transfer/Sharing
High	Reduce/Mitigate or Avoid

1. Risk Identification

The risk assessment process began with the identification of primary assets associated with the Let It Flo non-stop toll transaction system. This activity was conducted to determine the critical assets that support service operations and require protection. The identified primary assets are presented in Table 2.

Table 2. List of Primary Assets

Category	Code	Asset Name
Business Process	AU1	User Registration Business Process
	AU2	RFID Sticker Tag Ordering Business Process
	AU3	RFID Sticker Payment Business Process
	AU4	Account Synchronization Business Process
	AU5	Non-Stop Toll Transaction Business Process
Information	AU6	User Data
	AU7	Payment Data
	AU8	Vehicle Data
	AU9	Transaction History Data
	AU10	Non-Stop Transaction System Development Document
	AU11	Non-Stop Transaction System Operational Report Document

In addition to primary assets, supporting assets were identified to determine the resources that enable the operation of the Let It Flo system. These assets include hardware, software, communication networks, and personnel, as presented in Table 3.

Table 3. List of Supporting Assets

Category	Code	Asset Name
Hardware	AP1	Control Unit
	AP2	RFID Receiver Antenna
	AP3	Road Side Server
	AP4	Application Web Server
	AP5	Payment Gateway Server
	AP6	Transaction Data Server
	AP7	Database Server
	AP8	Temporary Data Server (Cache)
Software	AP9	Non-Stop Transaction Service Web Application

	AP10	Operating System: Linux Ubuntu
	AP11	Database System: MongoDB and PostgreSQL
	AP12	Supporting Application: Google Kubernetes Engine, Kafka, and Redis
Communication Network	AP13	Network Device: Router (Mikrotik)
	AP14	Internet Service
Personnel	AP15	Decision Maker
	AP16	System Developer
	AP17	Operational Team

Following the identification of primary and supporting assets, threat identification was conducted to determine potential threats that could disrupt the operation and performance of the Let It Flo system. This process aimed to identify events that may affect the confidentiality, integrity, and availability of the identified assets. The list of identified threats is presented in Table 4.

Table 4. Threat Identification

Category	Code	Threat
Physical Damage	T1	Fire
	T2	Accident Incident
Natural Event	T3	Destruction of equipment or media
	T4	Flood
Infrastructure Failure	T5	Loss of electrical power supply
	T6	Communication device malfunction
Technical Failure	T7	Device damage
	T8	Software malfunction
	T9	Disruption to information system maintenance
Human Action	T10	Remote eavesdropping
	T11	Theft of media or documents
	T12	Theft of hardware
	T13	Unauthorized use of devices
	T14	Use of unauthorized devices
	T15	Data corruption
	T16	Illegal data processing
Compromise of functions and services	T17	User error
	T18	Misuse of access rights
	T19	Repudiation
	T20	Violation of personnel availability

After identifying the relevant threats, potential impacts on the identified assets were determined to understand the possible consequences of threat occurrences. The combination of assets, threats, and impacts was then used to formulate risk scenarios that serve as the basis for subsequent risk analysis and evaluation activities. The identified impacts and risk scenarios are presented in Table 5.

Table 5. Impact and Risk Scenario Identification

Asset Type	Threat	Impact	Risk Code
Information			
User Data (AU6); Payment Data (AU7);	Remote eavesdropping (T10)	Decline in public trust or reputation	R1

Vehicle Data (AU8); Transaction History Data (AU9).	Data corruption (T15)	Disruption to internal and third-party operations	R2
	Illegal data processing (T16)	Violation of legal, regulatory, or statutory provisions; Decline in public trust or reputation	R3
Non-Stop Transaction System Development Document (AU10); Non-Stop Transaction System Operational Report Document (AU11).	Theft of media or documents (T11)	Violation of legal, regulatory, or statutory provisions; Decline in public trust or reputation	R4
Hardware			
Control Unit (AP1); RFID Receiver Antenna (AP2); Road Side Server (AP3); Application Web Server (AP4); Payment Gateway Server (AP5); Transaction Data Server (AP6); Database Server (AP7); Temporary Data Server (Cache) (AP8).	Fire (T1)	Disruption to internal and third-party operations	R5
	Accident incident (T2)	Disruption to internal and third-party operations	R6
	Flood (T4)	Disruption to internal and third-party operations	R7
	Loss of electrical power supply (T5)	Disruption to internal and third-party operations	R8
	Theft of hardware (T12)	Disruption to internal and third-party operations; impact on work plans and deadlines	R9
	Device damage (T7)	Disruption to internal and third-party operations	R10
	Unauthorized use of devices (T13)	Violation of legal, regulatory, or statutory provisions	R11
Software			
Non-Stop Transaction Service Web Application (AP9)	Software malfunction (T8)	Disruption to internal and third-party operations	R12
	Disruption to information system maintenance (T9)	Disruption to internal and third-party operations	R13
	User error (T17)	Disruption to internal and third-party operations	R14
	Misuse of access rights (T18)	Decline in public trust or reputation; Violation of legal, regulatory, or statutory provisions.	R15
Operating System: Linux Ubuntu (AP10)	Software malfunction (T8)	Disruption to internal and third-party operations	R16
	Use of unauthorized devices (T14)	Violation of legal, regulatory, or statutory provisions	R17
Database System: MongoDB and PostgreSQL (AP11)	Data corruption (T15)	Disruption to internal and third-party operations; Loss of business and financial value	R18
	Illegal data processing (T16)	Violation of legal, regulatory, or statutory provisions	R19
Supporting Application: Google Kubernetes Engine, NginX, Kafka, and Redis (AP12)	Software malfunction (T8)	Disruption to internal and third-party operations	R20

Communication Network			
Network Device: Router (Mikrotik) (AP13)	Communication device malfunction (T6)	Disruption to internal and third-party operations; Breach of contract or service level	R21
Internet Service (AP14)	Communication device malfunction (T6)	Disruption to internal and third-party operations; Breach of contract or service level	R22
Personnel			
Decision Maker (AP15); System Developer (AP16); Operational Team (AP17).	User error (T15)	Disruption to internal and third-party operations; Impact on work plans and deadlines	R23
	Illegal data processing (T16)	Violation of legal, regulatory, or statutory provisions	R24
	Violation of personnel availability (T20)	Loss of personnel and intellectual capital (expertise and competence); Disruption to internal and third-party operations Impact on work plans and deadlines.	R25
Organization			
JMTO Information Technology Directorate (AP18)	Misuse of access rights (T18)	Decline in public trust or reputation Violation of legal, regulatory, or statutory provisions	R26

2. Risk Analysis

Following the identification of risk scenarios, a risk analysis was performed to assess the likelihood and impact of each identified risk. The analysis was conducted using the established risk assessment criteria to determine the corresponding risk level and classification. The results of the risk analysis are presented in Table 6.

Table 6 Risk Analysis

Risk Code	Vulnerability	Likelihood Level	Impact Level	Risk Level
R1	Unprotected communication channel	C	4	18 (Moderate to High)
R2	Inadequate backup system	C	4	18 (Moderate to High)
R3	Incorrect access rights management	C	5	23 (High)
R4	Unprotected document storage	B	4	15 (Moderate to High)
R5	Inadequate physical protection of buildings	A	5	20 (High)
R6	Inadequate physical protection of buildings	B	4	15 (Moderate to High)
R7	Flood-prone location	A	4	15 (Moderate)
R8	Unstable power supply	C	4	18 (Moderate to High)
R9	Inadequate controls over device access	B	4	18 (Moderate to High)
R10	Inadequate maintenance	C	4	18 (Moderate to High)
R11	Absence of an authorization system for device use	A	3	10 (Low to Moderate)

R12	Inadequate system testing	B	4	16 (Moderate to High)
R13	Inadequate response to system disruption	C	3	13 (Moderate)
R14	Lack of user awareness in system operation	B	3	11 (Low to Moderate)
R15	Inadequate authentication mechanism	B	3	11 (Low to Moderate)
R16	Inadequate system testing	B	4	16 (Moderate to High)
R17	Unauthorized use of devices	B	3	11 (Low to Moderate)
R18	Inadequate backup system	C	5	23 (High)
R19	Incorrect access rights management	B	3	11 (Low to Moderate)
R20	Inadequate system testing	C	4	18 (Moderate to High)
R21	Inadequate maintenance	C	4	18 (Moderate to High)
R22	Absence of backup internet service	C	4	18 (Moderate to High)
R23	Lack of training and awareness in system usage	B	2	6 (Low to Moderate)
R24	Incorrect access rights management	B	3	11 (Low to Moderate)
R25	Absence of adequate personnel	B	3	11 (Low to Moderate)
R26	Incorrect access rights management	B	3	11 (Low to Moderate)

Following the risk analysis process, risk evaluation was conducted to determine the appropriate treatment decision for each identified risk. The evaluation was performed by comparing the calculated risk levels against the organization's risk evaluation and risk acceptance criteria. Based on this process, risks exceeding the acceptable threshold were designated for mitigation, while risks within the acceptable range were considered acceptable and subject to monitoring. The results of the risk evaluation are presented in Table 7.

Table 7. Risk Evaluation

Risk Code	Risk Level	Risk Evaluation
R3	High	Mitigation
R18	High	Mitigation
R5	High	Mitigation
R1	Moderate to High	Mitigation
R2	Moderate to High	Mitigation
R8	Moderate to High	Mitigation
R9	Moderate to High	Mitigation
R10	Moderate to High	Mitigation
R20	Moderate to High	Mitigation
R21	Moderate to High	Mitigation
R22	Moderate to High	Mitigation
R4	Moderate to High	Mitigation
R12	Moderate to High	Mitigation
R16	Moderate to High	Mitigation
R6	Moderate to High	Mitigation

R7	Moderate	Mitigation
R13	Moderate	Mitigation
R14	Low to Moderate	Accepted
R15	Low to Moderate	Accepted
R17	Low to Moderate	Accepted
R19	Low to Moderate	Accepted
R24	Low to Moderate	Accepted
R25	Low to Moderate	Accepted
R26	Low to Moderate	Accepted
R11	Low to Moderate	Accepted
R23	Low to Moderate	Accepted

Based on the risk evaluation results, a total of 26 risk scenarios were identified and evaluated. The results indicate that 3 risk scenarios were classified as High, 12 as Moderate to High, 2 as Moderate, and 9 as Low to Moderate. In accordance with the established risk acceptance criteria, 17 risk scenarios categorized as High, Moderate to High, and Moderate require mitigation measures to reduce their risk levels to an acceptable threshold. Meanwhile, the 9 risk scenarios classified as Low to Moderate fall within the organization's acceptable risk range and therefore do not require additional mitigation measures.

The risk evaluation results provide the basis for the subsequent risk treatment stage. In this study, risk treatment focuses on risk modification through the implementation of appropriate controls and mitigation measures to reduce the likelihood and impact of identified risks. The proposed treatment plans were developed by considering the characteristics of each risk scenario and by referencing the relevant controls specified in ISO/IEC 27002:2022. The recommended risk treatment actions for the identified risks are presented in Table 8.

Table 8. Risk Treatment

Risk Code	Treatment Action Plan	ISO 27002 Clause
R3	Implement centralized role-based access control (RBAC) and review access rights at least every 6 months	5.15 Access Control; 5.16 Identity Management
R18	Implement off-site backup mechanisms and disaster recovery testing	8.13 Information Backup; 5.30 ICT Readiness for Business Continuity
R5	Conduct periodic fire emergency response simulations and tests	5.29 Information Security During Disruption
R1	Add end-to-end encryption to all external communication channels and conduct periodic network penetration testing	8.20 Network Security; 8.21 Security of Network Services; 8.24 Use of Cryptography
R2	Conduct scheduled data recovery tests (restore tests) and document the results	8.13 Information Backup; 5.30 ICT Readiness for Business Continuity.
R8	Conduct periodic UPS and generator testing and record the test results	5.30 ICT Readiness for Business Continuity

R9	Conduct physical access audits and periodically review secure device zones	7.2 Physical Entry
R10	Develop device performance indicators and analyze failure trends	7.13 Equipment Maintenance
R20	Develop and test rollback procedures for supporting applications	8.32 Change Management
R21	Conduct periodic network device failover testing	8.20 Network Security
R22	Add a second ISP connection via a different route and conduct failover testing at least twice a year	5.30 ICT Readiness for Business Continuity; 8.21 Security of Network Services
R4	Implement information classification and role-based access restrictions	5.12 Classification of Information
R12	Add regression testing and security testing after system changes	8.29 Security Testing in Development and Acceptance
R16	Conduct compatibility testing and prepare a rollback plan before OS updates	8.32 Change Management
R6	Evaluate the effectiveness of signs, safeguards, and device locations	7.8 Equipment Siting and Protection
R7	Develop and test a post-flood recovery plan (disaster recovery scenario)	5.29 Information Security During Disruption
R13	Develop system maintenance SLAs and evaluate SLA compliance	5.36 Compliance with Policies, rulesand standards for infrormation security

CONCLUSION

Based on the results and discussions that have been conducted, this study concludes that the proposed information security risk management design for the non-stop toll transaction system at PT Jasamarga Tollroad Operator has successfully addressed the research objectives and questions that were previously established. The proposed design was developed based on the ISO/IEC 27005:2022 framework and encompasses the stages of context establishment, risk assessment, risk treatment, and risk acceptance. The context establishment stage was conducted by defining the scope, limitations, and risk management structure applied to the non-stop toll transaction services at JMTO, while the determination of risk management criteria was aligned with the organization's internal risk management policies. Furthermore, the risk assessment process consisted of risk identification, analysis, and evaluation activities, resulting in the identification of 26 risk scenarios. Among these scenarios, 3 risks were categorized as high level, 12 as moderate-to-high level, 2 as moderate level, and 9 as low-to-moderate level risks. Based on the organization's risk evaluation and risk acceptance criteria, 17 risk scenarios classified as high, moderate-to-high, and moderate required mitigation actions to reduce the overall risk level, while 9 low-to-moderate risk scenarios were considered acceptable and therefore did not require additional mitigation. The risk treatment process focused on risk modification strategies through the implementation of mitigation controls aimed at reducing both the likelihood and impact of each identified risk scenario. The proposed controls were developed in accordance with ISO/IEC 27001:2022 and its implementation guidance provided in ISO/IEC 27002:2022. Finally, the risk acceptance process was carried out through a review by the risk owners regarding the proposed treatment plans and the resulting residual risks after

mitigation. The acceptance decisions were determined based on JMTO's organizational risk acceptance criteria, ensuring that all residual risks remained within acceptable organizational thresholds.

REFERENCES

Alsaleh, A. (2025). Toward a conceptual model to improve the user experience of a sustainable and secure intelligent transport system. *Acta Psychologica*, *255*, 104892.

Ayo, S. C., Ngala, B., & Amzat, O. (2018). *Information security risks assessment: A case study*.

Burger, G., & Guna, J. (2024). Enhancing driving safety through user experience evaluation of the C-ITS mobile application: A case study of the Dars Traffic Plus app in a driving simulator environment. *Sensors, 24*(15), 4948.

Dimian, M., Zadobrischi, E., Căilean, A., Beguni, C., Avătămăniței, S.-A., & Paşcu, P. (2024). Digital transformation of the transport sector towards smart and sustainable mobility. In *Digital transformation: Technology, tools, and studies* (pp. 215–237). Springer.

Fatorachian, H., Kazemi, H., & Pawar, K. (2025). Digital transformation for sustainable transportation: Leveraging Industry 4.0 technologies to optimize efficiency and reduce emissions. *Future Transportation, 5*(2), 34.

Grigaliūnas, Š., Schmidt, M., Brūzgienė, R., Smyrli, P., Andreou, S., & Lopata, A. (2024). Holistic information security management and compliance framework. *Electronics, 13*(19), 3955.

Herath, T. C., Herath, H. S. B., & Cullum, D. (2023). An information security performance measurement tool for senior managers: Balanced scorecard integration for security governance and control frameworks. *Information Systems Frontiers, 25*(2), 681–721.

Hidayatullah, D. E. R., Kunthi, R., & Harwahyu, R. (2024). Design and analysis of information security risk management based on ISO 27005: Case study on Audit Management System (AMS) XYZ Internal Audit Department. *International Journal of Electrical, Computer, and Biomedical Engineering, 2*(3). https://doi.org/10.62146/ijecbe.v2i3.81

Huang, Y., Hu, M., Xu, J., & Jin, Z. (2023). Digital transformation and carbon intensity reduction in transportation industry: Empirical evidence from a global perspective. *Journal of Environmental Management, 344*, 118541.

International Organization for Standardization. (2022). *ISO/IEC 27005:2022 information security, cybersecurity and privacy protection—Guidance on managing information security risks*.

International Standard Organization. (2022a). *ISO/IEC 27001:2022 information security, cybersecurity and privacy protection—Information security management systems—Requirements*.

International Standard Organization. (2022b). *ISO/IEC 27002:2022 information security, cybersecurity and privacy protection—Information security controls*.

Irfan, M. N., Ramadhania, S., Hadi, S., & Pungkasanti, P. T. (2025). ISO/IEC 27005-based e-learning risk management with blockchain architecture: A case study of Semarang University. *Journal of Information Systems and Informatics, 7*(3), 2898–2919. https://doi.org/10.51519/journalisi.v7i3.1265

Islam, M. D. (2025). *Web-based real-time bus tracking system for enhanced commuter experience and efficient fleet management*.

Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk prediction for the critical infrastructure protection. *Neural Computing and Applications, 34*(18), 15241–15271.

Li, P., Xue, R., Shao, S., Zhu, Y., & Liu, Y. (2023). Current state and predicted technological trends in global railway intelligent digital transformation. *Railway Sciences, 2*(4), 397–

412.
Mujib, M. S. (2021). *Penilaian risiko keamanan informasi pada sistem informasi manajemen rumah sakit menggunakan kerangka kerja ISO/IEC 27005:2022*.
Muralidharan, V. (2025). The IoT-based toll gate management system. *ICNGTS*.
Nazari, Z., & Musilek, P. (2023). Impact of digital transformation on the energy sector: A review. *Algorithms, 16*(4), 211.
Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability, 15*(18), 13369.
Sharma, M., & P. C., A. (2013). A research survey: RFID security & privacy issue. *Computer Science & Information Technology*, 255–261. https://doi.org/10.5121/csit.2013.3526
Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview. *Electronics, 11*(14), 2181.
Verma, S. K., Verma, R., Singh, B. K., & Sinha, R. S. (2024). Management of intelligent transportation systems and advanced technology. In *Intelligent transportation system and advanced technology* (pp. 159–175). Springer.