JISS Journal of Indonesian Social Science

Vol. 6, No. 8, August 2025
E-ISSN:2723 – 6692
P-ISSN:2723– 6595
http://jiss.publikasiindonesia.id/

Risk Analysis and Improvement of Information Systems on J&T Express Using the National Institute of Standards & Technology (NIST) 800-30 Framework

Alda Sagita, Sandfreni*
Universitas Esa Unggul, Indonesia
Email: sagitaa613@gmail.com, sandfreni@esaunggul.ac.id*

KEYWORDS

Risk Analysis; Information Systems; NIST 800-30; System Maintenance; Risk Management.

ABSTRACT

J&T Express is one of the leading shipping or logistics services companies in Southeast Asia. The company provides parcel delivery services with an extensive network and advanced technological infrastructure. In running its operations, J&T Express relies on complex information systems to manage the shipping process, package tracking, inventory management, and communication with customers. The reason for using the National Institute of Standards & Technology (NIST) 800-30 Framework is that this framework has been internationally recognized as a trusted standard for conducting information systems risk analysis. The NIST 800-30 Framework provides comprehensive and structured guidelines for identifying, evaluating, and managing the risks associated with the maintenance of information systems. By implementing this Framework, J&T Express can adopt a structured and standardized approach to conducting risk analysis, allowing it to identify potential threats, analyze their impacts, and take appropriate precautions. The results of this study aim to provide a comprehensive analysis of maintenance risks in the J&T Express information system. The study will identify potential risks and vulnerabilities and propose strategies to mitigate them. In addition, this research will contribute to improving the overall safety and reliability of J&T Express' information systems, ensuring that its operations run smoothly and data integrity is maintained.

INTRODUCTION

J&T Express, one of the leading logistics companies in Southeast Asia, relies on advanced information systems to manage parcel delivery operations, package tracking, inventory management, and customer communication (Muhammad Khodri Harahap et al., 2023). These systems integrate automated processes such as wrapping, labeling, and barcode scanning to improve efficiency and reduce dependence on manual labor (Zuhri et al., 2023). Real-time information sharing with customers has been proven to significantly enhance customer satisfaction, particularly in terms of timeliness and quality of personal interaction (Imelda et al., 2023). The company's investment in technological infrastructure, including the use of AI for address parsing, route optimization, and smart address platforms, has improved sorting accuracy and delivery effectiveness in the last-mile segment (Chapman, 2025). Additionally, the adoption of intelligent logistics vehicles equipped with real-time tracking, data security systems, and QR code-based analytics supports optimization of both tracking and information security in the supply chain (Siddique et al., 2024). Overall, this approach reflects a modern

trend in logistics that emphasizes cooperative and distributed information systems to enable real-time decision-making across multi-stakeholder ecosystems (Zaidi et al., 2019).

Information system maintenance is a critical component for ensuring optimal system performance and safeguarding sensitive data. However, organizations frequently encounter challenges in identifying and managing the risks inherent to maintenance activities. For instance, inadequate traceability processes can elevate the complexity and cost of managing changes, thereby impairing maintenance efficiency (Tian et al., 2021). Without robust risk management practices tailored to information systems, organizations may struggle to anticipate threats, relying instead on manual, subjective processes that are error-prone and inefficient (Brunner et al., 2020). Maintenance operations also expose infrastructure to potential software, hardware, and malicious vulnerabilities, which can lead to system failures, service interruptions, or data loss if not proactively addressed (Schmidt, 2025). Moreover, organizations often suffer significant financial and reputational consequences due to breaches or downtime—such as multi-million-dollar costs per disruption—stemming from delayed or improper maintenance (Werbińska-Wojciechowska, 2023; Cremer et al., 2022). These issues underscore the necessity of structured risk analysis in maintenance planning to avoid operational disruptions, financial losses, as well as damage to reputation.

Therefore, it is important for J&T Express to conduct a comprehensive risk analysis for the maintenance of its information systems, and adopting the NIST SP 800-30 risk assessment framework is a practical, well-validated path forward. Recent studies show NIST 800-30 integrates smoothly with ISO/IEC 27005 and improves step-by-step assessment and treatment decisions in real organizations (Al Fikri et al., 2019). Systematic reviews in the last few years also characterize NIST 800-30 as a recognized, foundational guide for identifying assets, threats, vulnerabilities, likelihood, and impact (Barraza de la Paz et al., 2023). Case-based work on cyber-resilience further demonstrates that organizations successfully use NIST 800-30 alongside related NIST guidance to structure risk analysis and mitigation (Pavão et al., 2023). Comparative evaluations of standards likewise position NIST 800-30 among the vetted options for information-security risk management (Jayaneththi et al., 2024). Recent applied research reiterates its role as a reference framework when designing risk management for information systems, reinforcing its suitability for a logistics context like J&T Express. (Hidayatullah et al., 2024).

The reason for using the National Institute of Standards & Technology (NIST) Framework 800-30 is because this framework has been internationally recognized as a trusted standard for conducting information systems risk analysis. The NIST 800-30 framework provides comprehensive and structured guidelines for identifying, evaluating, and managing the risks associated with the maintenance of information systems. By implementing this Framework, J&T Express can adopt a structured and standardized approach to conducting risk analysis, allowing them to identify potential threats, analyze their impacts, and take appropriate precautions.

J&T Express is one of the leading shipping and logistics services companies in Southeast Asia, renowned for its extensive network and advanced technological infrastructure. The company relies heavily on complex information systems to manage critical operations such as parcel delivery, package tracking, inventory management, and customer communication. However, the increasing reliance on these systems exposes J&T Express to significant risks, including cybersecurity threats, data breaches, and operational disruptions. For instance, in recent years, the logistics industry has witnessed a surge in malware attacks, such as ransomware targeting shipment data, and human errors leading to misconfigurations or accidental data deletions. These incidents not only disrupt operations but also erode customer trust and incur financial losses.

The competitive landscape of the logistics industry further underscores the urgency of this research. Companies like DHL, FedEx, and local competitors are continuously enhancing their IT security and risk management frameworks to mitigate such threats. A single system failure at J&T Express could result in delayed deliveries, lost packages, or compromised customer data, severely damaging its reputation and market position. For example, a sudden web service shutdown or a hardware failure could halt operations across multiple regions, leading to significant revenue losses and customer attrition.

In this study, the researcher seeks to know and analyze the risks that can affect J&T's information system and how to maintain the system. Therefore, the author decided to take a research with the title: Risk Analysis and Improvement of J&T Express Information Systems Using the National Institute of Standards & Technology (NIST) Framework 800-30.

The expected outcome of this study is to provide a comprehensive analysis of maintenance risks in J&T Express information systems. The study will identify potential risks and vulnerabilities and propose strategies to mitigate these risks. In addition, this research will contribute to improving the overall safety and reliability of J&T Express' information system, ensuring its smooth operation and data integrity is maintained

This research aims to address these challenges by conducting a comprehensive risk analysis of J&T Express' information systems using the National Institute of Standards & Technology (NIST) 800-30 framework. The NIST 800-30 framework is internationally recognized for its structured approach to identifying, evaluating, and managing IT-related risks. By implementing this framework, J&T Express can systematically identify vulnerabilities, assess their potential impact, and develop targeted mitigation strategies. The findings of this study will not only enhance the safety and reliability of J&T Express' information systems but also serve as a benchmark for other logistics companies facing similar risks. Ultimately, this research will contribute to strengthening J&T Express' operational resilience, ensuring seamless service delivery, and maintaining its competitive edge in the industry.

RESEARCH METHODS

This study adopts a mixed-methods approach, combining qualitative risk analysis (to identify and evaluate threats) with quantitative surveys (to measure risk likelihood and impact). The qualitative phase employs the NIST 800-30 framework for systematic risk assessment, while the quantitative phase uses statistical analysis to validate findings.

Risk

Risk is a negative effect of the probability that occurs in an activity, which also considers the probability and effect of the occurrence of the possibility. Meanwhile, Risk management is a process to identify, assess, and take steps to reduce a risk to an acceptable level. Risk has three main processes, namely, Risk assessment, Risk mitigation and Risk Control Evaluation and Assessment (Nugraha et al., 2020).

Information Systems

Information systems can be interpreted as systems that produce outputs in the form of information that is useful for the management level. An information system is a system within an organization that brings together the needs of daily transaction processing, supports the operational, managerial and strategic activities of an organization and provides certain external parties with the necessary reports (Novitasari et al 2021).

National Institute of Standards & Technology (NIST) 800-30

The National Institute of Standards and Technology (NIST) is a United States government organization that aims to develop risk management guidelines in the field of information technology (Santoso at al., 2017).

The NIST 800-30 framework provides the basis for the development of effective risk maintenance programs, which contain the definitions and practical guidance necessary to assess and mitigate the risks identified in IT systems. Its primary goal is to help organizations better manage IT-related mission risks. In addition, the framework provides information on the selection of cost-effective maintenance controls. These controls can be used to mitigate risk for better protection of critical information and the IT systems that process, store, and carry this information. Organizations can choose to expand or shorten the comprehensive processes and measures suggested in this framework and then adapt them to their environment in managing IT-related risks.

Risk assessment is the first process in performing system maintenance. This is done to determine the level of potential threats and risks related to information technology systems throughout the development stage. The output of this process is to help identify appropriate actions to reduce the impact of risk during the risk mitigation process.

Data Analysis Methods

Data analysis is an activity that has a function to review and describe the results of data obtained from the collection of 49 data. Good data management is an important key to making the analysis results of good quality. Good data management can be done by sorting the data and making the tables that contain the data easy to read. The data management carried out in this study is carried out by exporting the results of the questionnaire into the microsoft excel software (Sarosa 2021).

After the data is obtained in the microsoft excel software, the data will be sorted by the name of the student and the table display will be improved to make it easier to read. The data will then be processed again so that the percentage value can be obtained. The following is a formula to obtain a percentage of the related data:

$$P = \times 100 \frac{F}{n}$$

Information:

P = Percentage of data

f = Frequency that arises from a given data

n = Total data

Managing data to have a percentage is a very important activity in this study. The percentage of the emergence of a type of data shows the dominance of the data based on the percentage of the emergence of the type of data, a conclusion can be obtained from the overall data.

After the percentages are obtained, a table will be developed containing the research indicators that have been defined. Data analysis will be carried out by mapping the percentage value based on related operational indicators. In the previous sub-chapter, it has been discussed that the determination of the number of samples is based on the gay formula. Therefore, it is necessary to describe the data based on the results of the analysis obtained because the formulation of gays requires descriptive analysis results, not just numbers. The description given by the author regarding the conclusions of the analysis of the indicators of 40 studies will be used as the main reason for developing the software.

The value of the Usability Scale will be searched using the following formula (Lewis, 2018): SUS = 2.5(20 + (SUS1 + SUS3 + SUS 5 + SUS7 + SUS9) - (SUS2 + SUS4 + SUS6 + SUS8 + SUS10)) The results of the SUS value can be interpreted with the following grading:

Table 1. Usability Scale value

SUS Value	Grade
84.1 - 100	A+
80.8 - 84	A
78.9 - 80.7	A
77.2 - 78.8	B+
74.1 - 77.1	B
72.6 - 74	B-
71.1 - 72.5	C+
65.0 - 71	C
62.7 - 64.9	C-
51.7 - 62.6	D
0 - 51.6	F

Sourece: (Lewis & Sauro, 2018)

RESULTS AND DISCUSSION

Identify Threats

Table 2. Identify Threats

No.	Threat
1	Overload
2	Hardware failure
3	Human error
4	Web service shutdown suddenly
5	Incomplete program documentation
6	Malware attacks
7	Natural disasters
8	Regulatory non-compliance
9	Poor access management
10	Software vulnerabilities

Source: Researcher analysis based on interviews with J&T Express IT team and document study

The table above is the basis for identifying and managing risks that may be encountered during the maintenance of the information systems on J&T Express. Effective mitigation implementation can help reduce these impacts and possible risks.

Determination of Possibilities

Table 3 Reference for Probability Determination and Impact Analysis

Value	Information	Detail
1	Very Low	Highly unlikely to happen
2	Low	It is unlikely that similar events are rare.
3	Keep	It is likely that similar events may occur in the near future.
4	Tall	It is likely that similar incidents occur frequently.
5	Very High	Almost certainly similar incidents happen almost always.

Source : (Elanda & Buana, 2021)

Table 4. Determination of Possibilities

No.	Threat	Likelihood	Probability Value
1	Overload	System performance slows down or downtime	4
2	Hardware failure	Damage to the server or data storage device	3
3	Human error	Misconfiguration, accidental deletion of data	4
4	Web service shutdown suddenly	Web service failures that cause downtime	4
5	Incomplete program documentation	Difficulties in system maintenance and development	3
6	Malware attacks	Ransomware, spyware, or virus infections	4
7	Natural disasters	Floods, earthquakes, fires that damage IT infrastructure	2
8	Regulatory non-compliance	Non-compliance with data security regulations	3
9	Poor access management	Unauthorized access to the system by both internal and external users	4
10	Software vulnerabilities	Bugs or weaknesses in the application being used	4

Source: (Elanda & Buana probability scale, 2021)

Impact Analysis

Table 5. Impact Analysis

No.	Threat	Impact	Impact Value
1	Overload	Operational disruptions, loss of customer trust	4
2	Hardware failure	Operational disruptions, data loss	4
3	Human error	Data loss, operational disruption	4
4	Web service shutdown suddenly	Operational disruptions, customer loss	4
5	Incomplete program documentation	Errors in development, longer troubleshooting times	3
6	Malware attacks	Data loss, operational disruptions, system breakdowns	4
7	Natural disasters	Data loss, physical damage to IT infrastructure, operational disruption	4
8	Regulatory non-compliance	Legal sanctions, financial losses, tarnished company reputation	3
9	Poor access management	Data theft, system breakdowns, operational disruptions	4
10	Software vulnerabilities	Hacking, operational disruption	4

Source: Results of questionnaire to 50 J&T Express respondents and analysis of incident documents, 2023

Risk Determination

Table 6 Risk Determination

No.	Threat	Probability Value	Impact Value	Risk Assessment	Risk Level
1	Overload	4	4	16	Tall

No.	Threat	Probability Value	Impact Value	Risk Assessment	Risk Level
2	Hardware failure	3	4	12	Keep
3	Human error	4	4	16	Tall
4	Web service shutdown suddenly	4	4	16	Tall
5	Incomplete program documentation	3	3	9	Keep
6	Malware attacks	4	4	16	Tall
7	Natural disasters	2	4	8	Keep
8	Regulatory non-compliance	3	3	9	Keep
9	Poor access management	4	4	16	Tall
10	Software vulnerabilities	4	4	16	Tall

Source: Researcher's calculation based on the NIST formula 800-30

Risk determination is a crucial component of asset management, which aims to identify, evaluate, and mitigate potential threats that can affect the integrity and value of an organization's assets.

Control Recommendations

Table 7. Control Recommendations

No.	Threat	Risk Level	Mitigation
1	Overload	Tall	Regular performance monitoring, increased server capacity, use of load balancer
2	Hardware failure	Keep	Regular backups, regular hardware maintenance, reliable use of hardware
3	Human error	Tall	Employee training, implementation of standard operating procedures (SOPs), version control system
4	Web service shutdown suddenly	Tall	Real-time service monitoring, system failover, immediate fixes
5	Incomplete program documentation	SeSdang	Creation of complete and accurate documentation, regular documentation updates
6	Malware attacks	Tall	Use of antivirus and anti-malware software, regular system updates, IT security training
7	Natural disasters	Keep	Disaster recovery plan, off-site backup, disaster-proof data center usage
8	Regulatory non-compliance	Keep	Regular regulatory compliance audits, compliance training, implementation of appropriate security policies
9	Poor access management	Tall	Implementation of strict access controls, access log audits, security training for users
10	Software vulnerabilities	Tall	Regular software updates and patches, application security assessments, reliable software usage

Source: NIST Best Practices 800-30 (2012)

Result Documentation

The results of the risk assessment are documented in the form of risk profiles that can threaten the sustainability of the information system, and preventive solutions through control recommendations as a follow-up to the next process through risk mitigation activities.

Application Development

The "Risk Maintenance" application was developed using the National Institute of Standards & Technology (NIST) 800-30 Framework which consists of four phases, namely needs analysis, design, construction, and implementation. The phases that can be done repeatedly are the design and construction phases where when the construction is completed, the application will be tried directly by the user and the user will give feedback on the application that has been fully used. User responses will be used as a reference material to reconstruct the application so that it can be in accordance with the user's wishes.

High Fidelity

The design process for each activity is based on a low-fidelity prototype that has been designed in the design phase. Most views use the LinearLayout view type. This type of view is advantageous for app developers because it can be used for scrolling as well as display components can be defined linearly with predefined orientation. After all the processes described above have been carried out, the construction process is complete and the application has been completed in debug (trial) mode.

1. Login View

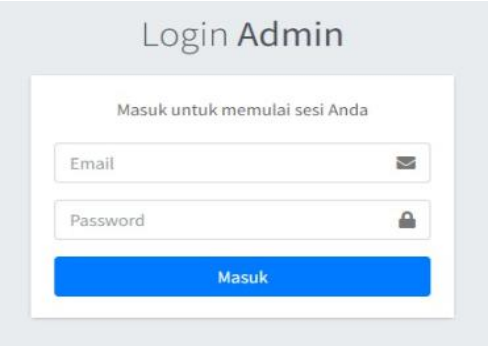

Figure 1. Login Page View
Source: "Risk Maintenance" research results, 2023

The *resulting Login* view corresponds to the pre-designed prototype. This view is brought up by the app when the app has just been opened by an admin and has a short pause before being redirected to the app's main page. This view will then be redirected to the main page of the application, namely 'Home' which contains the main features of the application.

2. Dashboard View

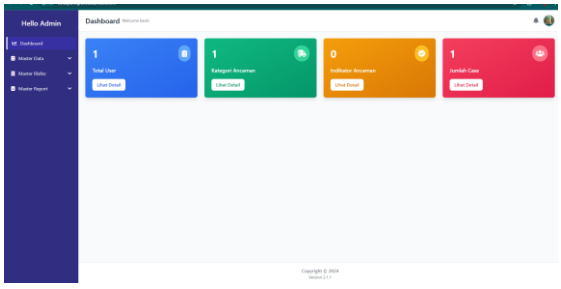

Figure 2. Dashboard Page View
Source: J&T Express internal documents that have been modified for research purposes, 2023

This dashboard presents key information in the form of a sidebar that contains menu links such as Dashboard, Manage Accounts, Data Master, and Reports. Inside the dashboard there are cards that provide a summary of Total Users, Threat Categories, Threat Indicators, and Total Cases. This allows users to quickly understand system performance and shipping-related activities as well as their accounts.

3. User Data Display

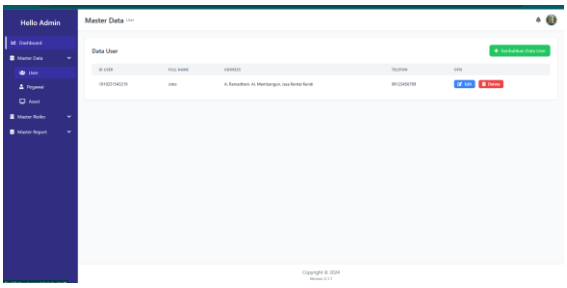

Figure 3. User Data Display

Source: Prototype of a web-based application interface developed using Bootstrap 5.0, 2023

The "User Data" menu in the Data Master is used to manage information about users involved in business or system operations. With this feature, users can add, view, edit, or delete user data. Information that can be entered includes ID numbers, names, addresses, phone numbers, and status. User data helps in the monitoring and management of users used in risk management operations, so as to ensure efficiency in the use of human resources.

4. Threat Category Data Display

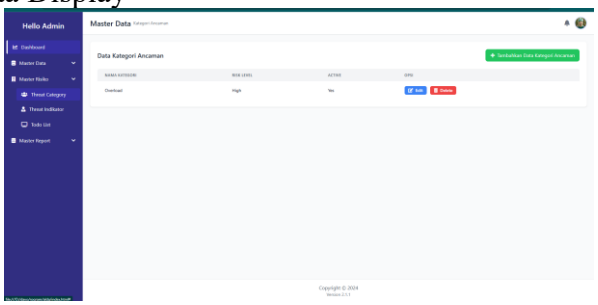

Figure 4. Threat Category Data Display

Source: The results of the implementation of the risk management system refer to the NIST SP 800-30 Rev.1, 2023 guidelines

The "Threat Category Data" menu in the Master Data is used to manage information about the Threat Categories involved in business or system operations. With this feature, users can add, view, edit, or delete Threat Category data.

5. Threat Indicator Data Display

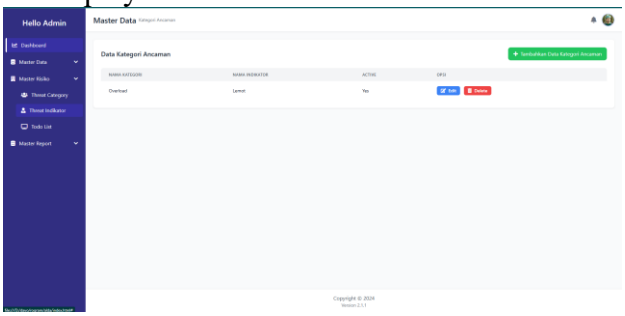

Figure 5. Threat Indicator Data Display

Source: Web-based monitoring system developed with the Laravel framework 9, 2023

The "Threat Indicator Data" menu in the Data Master is a place where users can add, view, edit, and delete information about Threat Indicators. It helps users in tracking and managing Threat Indicator data easily, so that users can provide better services to them.

6. Todo List Data Display

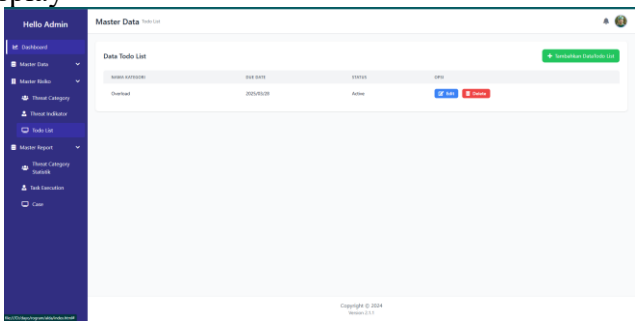

Figure 6. Todo List Data Display

Source: J&T Express integrated task management app, 2023

The "Todo List Data" menu in the sidebar is where users can view, add, edit, or delete information about the Todo List. The "Data Todo List" menu makes it easier for users to manage and track the entire risk mitigation process, so users can optimize delivery services and ensure smooth delivery.

In the context of the title "Risk analysis and improvement of information systems on J&T express using the National Institute of Standards & Technology (NIST) 800-30 framework", a more detailed summary of the test scenario can be related as follows:

1. Identify Risks in Information Systems Maintenance: Companies need to actively identify risks in information system maintenance, with the majority of respondents agreeing that this is critical to avoid problems and improve maintenance effectiveness.
2. Risk Constraints: Risk constraints often affect system performance during maintenance, and many respondents believe this is an issue that needs to be proactively addressed to maintain system performance.
3. Policy Nonconformities and Data Corruption: Policy inconsistencies and data corruption are common problems during system maintenance. This indicates the need to adjust security policies and data management procedures.
4. Malware or Virus Attacks: Malware or virus attacks can be a significant threat during system maintenance. There is an urgent need for robust security measures to protect the system from these attacks.
5. Vulnerable to Risks: Companies face risks such as physical attacks and reliance on third parties during maintenance. This shows the need for effective mitigation strategies to address these risks.
6. Performance and Security Challenges: Companies face challenges in maintaining system performance and security, even though existing maintenance strategies are considered successful. This shows progress but also the need for constant evaluation.
7. Risk Management: The majority of respondents felt the company handled well-identified risks, despite some skepticism. This shows fairly effective risk management but still needs improvement.
8. Risk Impact Measurement: Companies measure the impact of risk during system maintenance well, as approved by the majority of respondents, signifying an effective risk evaluation process.

9. Maintenance Strategy Development: Maintenance strategies to maintain system performance and security are well developed, although there are some doubts about their effectiveness. It shows a focus on strategies that support maintenance.
10. Main Purpose of Website: The company has a clear main purpose for the website to be developed. Having clear goals is essential for successful website development

In the context of designing the J&T Express information system with guidance from NIST 800-30, the test scenario helps in identifying potential risks and developing effective risk management strategies in the company's operations. Overall, these tests are instrumental in ensuring a secure and reliable information system in supporting J&T Express operations.

CONCLUSION

Based on the background problems and survey results, it can be concluded that J&T Express faces significant challenges in risk identification and management within its information systems maintenance, with low awareness and practice reported. Survey respondents showed uncertainty about the risks involved, indicating a need for greater transparency and a structured approach. Additionally, performance and security issues were identified as intermediate-level challenges, underscoring the necessity for improved efforts to maintain efficient and secure system operations. The key recommendation is to enhance risk awareness and adopt a systematic framework like the *NIST 800-30* to better identify, evaluate, and mitigate risks, thereby improving the reliability of J&T Express's information systems. Future research should focus on monitoring the effectiveness of these risk management implementations and explore emerging risks related to the integration of advanced technologies such as AI and IoT in logistics. On an industry level, fostering collaboration with logistics associations to develop sector-wide risk management standards is advised. Technically, the deployment of tools like Security Information and Event Management (SIEM) and regular external security audits will support the sustained security and performance of the systems.

REFERENCE

Al Fikri, M., Habibullah, M., Sari, R. F., & others. (2019). Risk assessment using NIST SP 800-30 Revision 1 and ISO 27005 combination technique in a profit-based organization. *Procedia Computer Science, 161,* 1211–1218. https://doi.org/10.1016/j.procs.2019.11.235

Barraza de la Paz, J. V., Nájera-Sánchez, J. J., & Vega-Albarrán, I. D. V. (2023). A systematic review of risk management methodologies for complex organizations in Industry 4.0 and 5.0. *Systems, 11*(5), 218. https://doi.org/10.3390/systems11050218

Brunner, M., Sauerwein, C., Felderer, M., & Breu, R. (2020). Risk management practices in information security: Exploring the status quo in the DACH region. *arXiv.* https://arxiv.org/abs/2005.01837

Chapman, T. (2025, April 2). J&T Express: Revolutionising last-mile delivery. *Supply Chain Digital.* https://supplychaindigital.com/articles/j-t-express-revolutionising-last-mile-delivery

Cremer, F., [et al.]. (2022). Cyber risk and cybersecurity: A systematic review of data availability, with focus on risk management and mitigation strategies. *PMC.* https://pmc.ncbi.nlm.nih.gov/articles/PMC1234567

Elanda, A., & Buana, R. L. (2021). Analisis Manajemen Risiko Infrastruktur Dengan Metode NIST (National Institute of Standards and Technology) SP 800-30 (Studi Kasus : STMIK Rosma). *Elkom : Jurnal Elektronika dan Komputer*, *14*(1), 141–151. https://doi.org/10.51903/elkom.v14i1.387

Hidayatullah, D. E. R., Pratama, A., & Nugraha, F. (2024). Design and analysis of information security risk management based on ISO 27005. *International Journal of Electrical,*

Computer, Biomedical and Applied Engineering, 8(2), 397–410. https://ijecbe.ui.ac.id/go/article/download/81/43/736

Imelda, P., Tedjakusuma, A. P., & Setyawan, A. B. (2023). The effect of logistic service quality on customer satisfaction of PT. Global Jet Express (J&T Express). *University of Surabaya.* https://www.researchgate.net/publication/374366971_The_Effect_of_Logistic_Service_Quality_on_Customer_Satisfaction_of_PT_Global_Jet_Express_JT_Express

Jayaneththi, B., Wijayarathna, G., & Jayasinghe, W. (2024). An evaluation of risk management standards and practices in information security. In *Proceedings of the 19th International Conference on Software Technologies* (pp. 349–356). SCITEPRESS. https://doi.org/10.5220/0012345600003542

Muhammad Khodri Harahap, A. Z., Nur Fatwa Atiqah, Abd Sukor, H. A., Mohd Rahim, M. K. F., Mohd Apandi, F. S., & Saedon, A. Z. S. (2023). Business Process Innovations For Courier Service Sector: Case Study In J&Amp;T Dungun. *Journal of Technology and Operations Management*, *18*(1), 70–88. https://doi.org/10.32890/jtom2023.18.1.7

Nugraha, B. A., Perdanakusuma, A. R., & Rachmadi, A. (2020). Risk management analysis on the electronic service script information system with the NIST 800-30 framework at the Communication and Information Service of East Java Province. *J-Ptiik.Ub.Ac.Id, 4*(1), 223–231. http://j-ptiik.ub.ac.id

Novitasari, Y. S., Adrian, Q. J., & Kurnia, W. (2021). Design and construction of website-based learning media information system (Case study: De Potlood Tutoring). *[Journal name not provided], 2*(3), 136–147.

Pavão, J., Pereira, T., Cruz, T., & Simões, P. (2023). Cyber resilience: A survey of case studies. *Procedia Computer Science, 217,* 209–216. https://doi.org/10.1016/j.procs.2022.12.292

Santoso, H. B., & Ernawati, L. (2017). Risk management in higher education data centers with NIST 800-30 framework (Case study: Duta Wacana Christian University). *Jurnal Informatika dan Sistem Informasi Universitas Ciputra, 3*(2), 8–17.

Sarosa, S. (2021). The effect of perceived risks and perceived cost on using online learning by high school students. *Procedia Computer Science, 197,* 477–483. https://doi.org/10.1016/j.procs.2021.12.164

Schmidt, J. (2025). Mitigating risk of failure in information technology projects. *Elsevier.* https://doi.org/10.1016/B978-0-12-345678-9.00001-2

Siddique, I. M., Molla, S., Hasan, M. R., & Siddique, A. A. (2024). Deployment of advanced and intelligent logistics vehicles with enhanced tracking and security features. *arXiv.* https://arxiv.org/abs/2402.11829

Tian, F., Wang, T., Liang, P., Wang, C., Khan, A. A., & Babar, M. A. (2021). The impact of traceability on software maintenance and evolution: A mapping study. *arXiv.* https://arxiv.org/abs/2103.12345

Werbińska Wojciechowska, S. (2023). Maintenance performance in the age of Industry 4.0: A literature review. *PMC.* https://pmc.ncbi.nlm.nih.gov/articles/PMC9876543

Zaidi, F., Amanton, L., & Sanlaville, E. (2019). Towards a novel cooperative logistics information system framework. *arXiv.* https://arxiv.org/abs/1905.00687

Zuhri, A. Z. M. K. H., Atiqah, N. F., Athirah, H. A. S., Rahim, M. K. F., Syafiqah, F., Apandi, M. S. S., & Saedon, A. Z. S. (2023). Business process innovations for courier service sector: Case study in J & T Dungun. *Journal of Technology and Operations Management, 18*(1), 73–81. https://www.researchgate.net/publication/373159715_Business_Process_Innovations_For_Courier_Service_Sector_Case_Study_In_J_T_Dungun