DOI: 10.33197/justinfo.v2i2.2534 ISSN: 3031-3449

A Case Study on Risk Management Implementation in the STNKGO Application Based on the NIST Framework

[1]Faza Nurfai'zi, [2]Leodry Bagus Sugiarso, [3]Muchamad Rusdan
[1,2]Sistem Informasi, Fakultas Teknik, Universitas Widyatama, Bandung, Indonesia
[3]Teknik Informatika, Fakultas Industri Kreatif, Universitas Teknologi Bandung, Bandung, Indonesia
[1]nurfaizi.faza@widyatama.ac.id, [2]leodry.bagus@widyatama.ac.id, [3]muchamad.rusdan@gmail.com

ABSTRACT

This research focuses on assessing and managing information technology risks in the STNKGO application, an online platform for payment and delivery of Vehicle Registration Certificates (STNK). Using the NIST SP 800-30 Revision 1 framework, the study systematically identifies, evaluates, and mitigates risks related to the application's operations. The assessment begins with identifying critical IT assets, including user data, vehicle registration records, transaction details, delivery information, and system software. Potential threats—such as cyberattacks, unauthorized access, and malware—are then analyzed alongside existing system vulnerabilities that could be exploited. Each risk is evaluated based on its likelihood and potential impact, allowing for classification by severity level. The study further examines current control measures and suggests enhancements, especially for mitigating high-risk scenarios involving cybersecurity threats. The findings highlight the necessity of implementing stronger data protection, enhancing system resilience, and reinforcing preventive controls. Applying the NIST SP 800-30 Revision 1 framework enables STNKGO to develop a structured and effective risk management strategy, ensuring improved security, reduced vulnerabilities, and greater continuity of services. This research contributes to the growing body of knowledge on IT risk management for digital public services, offering practical insights for enhancing the safety and reliability of online applications handling sensitive data and transactions.

Keywords: Risk Management, NIST Framework, Web Application, Mobile Application, Information Security.

Corresponding Author:

Faza Nurfai'zi
Sistem Informasi, Fakultas Teknik, Universitas Widyatama
Bandung, Indonesia
nurfaizi.faza@widyatama.ac.id

INTRODUCTION

In today's rapidly evolving digital era, the integration of technology into public services has become both a necessity and an opportunity for innovation. Governments and private institutions alike are adopting digital platforms to improve service delivery, efficiency, and user satisfaction. One such innovation in Indonesia is the STNKGO application, a web- and mobile-based system designed to facilitate the online payment and delivery of Vehicle Registration Certificates (Surat Tanda Nomor Kendaraan or STNK). This application represents a transformative shift from manual, time-consuming procedures to a more streamlined, user-friendly digital experience. However, the transition to online services also brings new challenges—most notably, the need to ensure robust information technology (IT) risk management.

Effective IT risk management is critical in the digital landscape. As online applications handle increasingly sensitive data and facilitate essential transactions, they become prime targets for cyber threats. The consequences of security breaches can be far-reaching, ranging from financial losses to identity theft, loss of public trust, and even disruption of public services. Therefore, the security, confidentiality, and integrity of the data handled by applications such as STNKGO must be safeguarded through structured, proactive, and adaptable risk management strategies.

This journal focuses on the implementation of IT risk management in the STNKGO application, with particular reference to the NIST SP 800-30 Revision 1 framework, a widely adopted guideline for conducting risk assessments in information systems. The study explores how this framework can be effectively applied to identify, analyze, and mitigate the specific risks faced by STNKGO as a digital platform operating in a public sector context. Through this approach, the study aims to contribute to the growing discourse on digital security governance and to provide a case study that may serve as a reference for similar applications in Indonesia and beyond.

The STNKGO application, while offering significant convenience, also processes a wide range of sensitive user information. This includes personal identity data (e.g., full name, date of birth, address, national ID number), vehicle information (e.g., registration number, ownership status), and payment details (e.g., credit/debit card numbers, CVV codes, transaction histories). Such data is highly valuable to malicious actors and must therefore be protected through secure data handling practices and comprehensive risk management. The exposure of this information due to poor security controls could result in legal consequences, financial harm to users, and reputational damage to the public authorities responsible for the system.

Furthermore, the increasing number of data breaches reported globally highlights the urgency of the issue. According to cybersecurity reports, millions of user records are compromised annually due to misconfigured servers, outdated software, and unpatched vulnerabilities. Public sector systems, particularly those transitioning from legacy infrastructures, are often unprepared for modern cyber threats. As such, the implementation of security frameworks like NIST becomes essential not just as a compliance measure, but as a strategic necessity.

In the case of STNKGO, key risk areas include the inadequate storage and management of payment data, which may fall short of compliance with international standards such as the Payment Card Industry Data Security Standard (PCI DSS). The application must ensure that payment information is stored securely using encryption and tokenization techniques, and that only authorized personnel have access to sensitive components. Moreover, data retention and deletion policies must align with Indonesia's Personal Data Protection (PDP) Act, ensuring that user information is not retained longer than necessary and is deleted securely upon request or expiration.

Another central concern is the risk of unauthorized transactions. As online financial transactions become more common, so too does the threat of fraud and identity theft. Weaknesses in authentication methods—such as reliance on static passwords or insufficient user verification—can lead to unauthorized access, manipulation of records, and fraudulent payments. This risk is amplified in systems like STNKGO, where real-time transaction processing is critical and the impact of a breach could affect thousands of users in a short span of time.

To address this, the study evaluates the existing authentication and verification mechanisms within the application. This includes reviewing the use of one-time passwords (OTPs), biometric authentication, session timeout configurations, and anomaly detection systems for suspicious activities. Furthermore, the application's ability to monitor and log user activities is assessed, ensuring that all transactions are traceable and auditable in case of security incidents.

Against this backdrop, the NIST SP 800-30 Revision 1 framework is employed as the foundation for the risk assessment conducted in this study. The framework provides a structured methodology for identifying IT assets, threats, vulnerabilities, and the potential consequences of risk events. The process includes four major components: risk framing, risk assessment, risk response, and risk monitoring. Within this context, the research focuses on the assessment phase, which involves determining the likelihood and impact of identified risks, as well as recommending appropriate mitigation strategies.

The use of the NIST framework is especially relevant for public sector applications because it promotes a holistic and continuous approach to risk management. It encourages system administrators and stakeholders to not only implement technical controls but also to understand the business and operational context of the system. This includes evaluating legal requirements, assessing user behavior, and anticipating emerging threats. By following this methodology, the STNKGO project

can move beyond reactive problem-solving and instead adopt a preventive and adaptive security posture.

The objectives of this research are threefold To identify the major IT risks associated with the operation of the STNKGO application, particularly those related to data privacy, payment security, and unauthorized system access. To evaluate the current risk controls and determine the extent to which they align with best practices outlined in the NIST SP 800-30 Revision 1 framework. To propose strategic recommendations for strengthening the application's risk management capabilities, ensuring better protection of users and system assets while supporting sustainable public service delivery.

The scope of this research is limited to the technical and procedural aspects of the STNKGO system. While the research touches on legal and policy compliance (such as the PDP Act and PCI DSS), it does not provide a full legal review. Likewise, the research does not focus on the user experience (UX) or user interface (UI) design of the application, except insofar as these relate to security features such as authentication workflows.

In conclusion, the importance of this study lies in its potential to inform digital service development in the Indonesian public sector, where digital transformation is often hindered by inadequate planning around cybersecurity. By presenting a case study that applies a globally recognized risk management framework to a real-world application, this research aims to bridge the gap between policy, technology, and implementation. The findings from this study are expected to offer valuable insights for system developers, government decision-makers, and cybersecurity professionals who are tasked with ensuring the safety and trustworthiness of online public services in Indonesia and similar environments.

LITERATURE REVIEW

Risk Management

Risk is related to uncertainty, it occurs because of the lack or unavailability of sufficient information about what will happen. Something that is uncertain can result in benefits or losses. Risk is a danger, consequence or consequence that can occur as a result of an ongoing process or future event, or can be interpreted as a state of uncertainty, where if an undesirable situation occurs it can cause loss. According to Ucu and Rozahi (2019) Risk is a danger, result, or consequence that can occur as a result of an ongoing process or future event, or can be interpreted as a state of uncertainty, where if an undesirable situation occurs it can cause losses. According to Sudarmanto et al. (2021), risk is an event that has not (possibly) occurred but has the potential to affect certain goals. The impact of the event can be positive or negative. According to Latifiana (2016), risk is the possibility of an adverse event occurring for a company or business, where the event cannot be predicted. According to Sidik and Wahyuari (2023), risk can generally be explained as uncertainty related to potential financial losses or the possibility of losses. This uncertainty can come from various factors, such as uncertainty in economic conditions, natural conditions, accidents, criminal acts such as murder or theft, and so on. According to Arifudin et al. (2020), risk can be interpreted as an event that results in losses or differences in results from those expected[1].

Risk management has become a very important aspect in various fields such as finance, business, technology, health, environment, and others. This concept focuses on identifying, assessing, and managing risks associated with the activities or operations of an entity. In management literature, risks can be categorized into several types, including financial, operational, reputational, and strategic risks. The importance of risk management is increasing along with the dynamic changes in the business environment and the complexity of the challenges faced by modern organizations. Organizations face a variety of risks that can interfere with achieving their goals, including financial risks related to market fluctuations, operational risks related to human error or system failures, as well as reputation risks that can affect public image and trust[2].

Web and Mobile Application

According to Aziz and Wulandari (2024) Web applications is serve as platforms for information dissemination and service provision, such as the promotional website for cafés that allows customers to view menus and place orders online[3]. According to Sánchez-Fernández et al. (2023) Mobile applications is offer real-time functionalities, such as the OITcontrol app for monitoring food allergies, which enables users to record and manage treatment responses efficiently[4].

According to Aronov (2023) Despite their benefits, the rapid evolution of technology presents challenges, including data security concerns and the need for digital literacy among users[5]. According to Rahmat et al. (2024) Additionally, the effectiveness of applications can vary based on user engagement and infrastructure support[6]. In contrast, while web and mobile applications offer significant advantages, their implementation can be hindered by issues such as user resistance to new technologies and the complexities of maintaining data security standards.

Framework NIST SP 800-30 Revision 1

The NIST Special Publication 800-30 Revision 1, titled "Guide for Conducting Risk Assessments," is a pivotal document that provides comprehensive guidance for conducting risk assessments of federal information systems and organizations. Published in 2012 by the National Institute of Standards and Technology (NIST), this publication aims to enhance the security and resilience of information systems through a structured approach to risk management[7]. The publication outlines a structured approach to risk assessment, which includes three main steps: preparing for the assessment, conducting the assessment, and maintaining the assessment. This process ensures that risk assessments are thorough and systematic, providing valuable insights for decision-makers[8].

The publication provides guidance on identifying and implementing appropriate security controls to mitigate identified risks. It also discusses the importance of residual risk management and the cost-benefit analysis of implementing security measures[9]. NIST SP 800-30 is widely used by federal agencies and organizations to conduct risk assessments and develop risk management strategies. Its structured approach and comprehensive guidelines make it a valuable resource for ensuring the security and integrity of information systems[10]. NIST SP 800-30 Rev-1 has established a risk assessment scale to facilitate the determination of risk levels, the following is a reference table in risk assessment:

Table 1. Adversial Likelihood Scale

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

Table 2. Non-Adversial Likelihood Scale

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times a year**.
High	80-95	8	Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times a year**.
Moderate	21-79	5	Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times a year**.
Low	5-20	2	Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year**, but **more than once every 10 years**.
Very Low	0-4	0	Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**.

Table 3. Impact Determination

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Table 4. Risk Determination Matrix

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

The risk assessment table is used to:

1. Standardize risk assessments
2. Ensure consistency in evaluation
3. Assisting in decision-making related to risk mitigation
4. Prioritizing remedial actions based on risk level

METHODOLOGY

The research flow based on NIST SP 800-30 Revision 1 starts with the preparation phase, where the scope and purpose of the risk assessment are defined, including identifying the relevant IT assets, systems, and processes involved, as well as determining the stakeholders and their roles. The next step is the risk assessment phase, which includes identifying potential threats that could impact the system, identifying vulnerabilities that could be exploited by these threats, determining the likelihood of each threat occurring, and assessing the potential impact if those threats were to materialize. This leads to evaluating the overall risk by combining the likelihood and impact, classifying the risks into categories such as low, moderate, or high. In the control recommendations phase, appropriate mitigation strategies are identified for each risk.

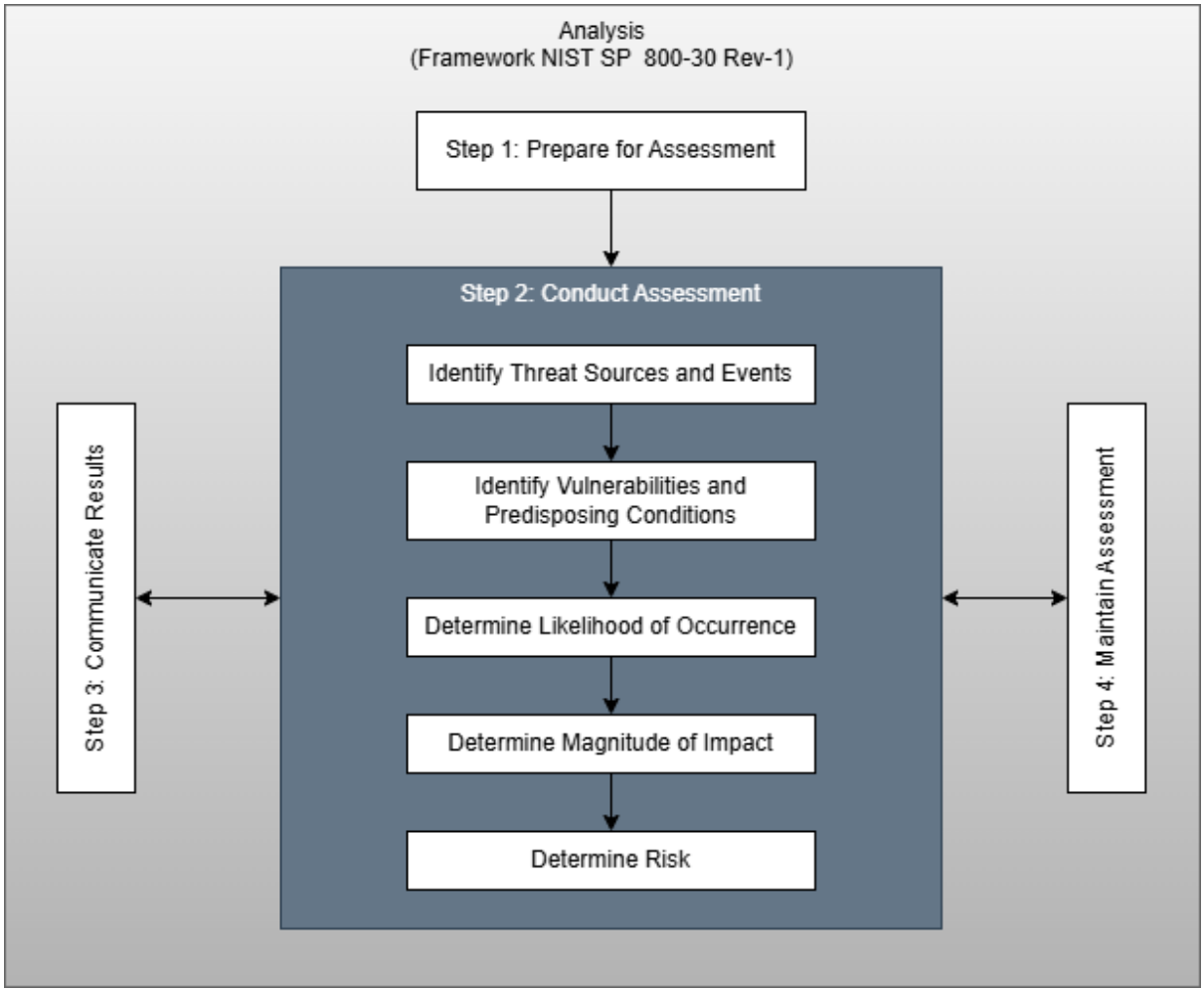

Figure 1. Research Flow

RESULT AND DISCUSSION

Identify Assets

The phase of implementing IT risk management in the STNKGO system utilizing the NIST SP 800-30 Revision 1 framework, begins with the identification of IT assets that are important to the firm. Our findings and literature assessments from various periodicals indicate that STNKGO possesses several identifiable IT assets.

Table 5. Asset Identifications

Asset Categories	Assets	Asset Code
Data	Personal Data	D1
	Vehicle Registration Certificate	D2
	Transaction Data	D3
	Delivery Data	D4
	Log Activity Data	D5
Software	Frontend Application	S1
	Application Programming Interface	S2

	Payment Gateway	S3
	Database	S4
	Firewall	S5
	Email System	S6
Hardware	Cloud Server	H1
	Computer	H2
Human Resources	User	HR1
	Admin	HR2
	Courier	HR3
	IT Developer	HR4

1. Asset Category: A type or group of assets, such as data, hardware, software, or human resources (HR).
2. Asset: The asset's name.
3. Asset Code: A unique code that identifies every object.

Identify Threat Sources and Events

During this phase, several threat sources may interrupt or harm STNKGO's important IT assets. Knowing the list of threat sources in IT assets will make it easier for STNKGO to develop control measures to reduce losses. The Threat Source Identification Table displays a list of potential risks to STNKGO's IT assets.

Table 6. Identify Threat Sources

Threat Sources	Threat	Threat Code	Asset Codes
Environment	Wildfire	TE1	H1, H2, HR1-HR4
	Power Outages	TE2	H1, H2
	Network Disruption	TE3	S1-S6
Human	Operator Error	TH1	D1-D5
	Cyber Attack	TH2	D1-D5, S1-S6
	User Irresponsibility	TH3	HR1-HR4
Virus	Malware	TV1	S1-S6
	Ransomware	TV2	D1-D5

1. Environment: Environment conditions that may interrupt or harm the system.
   a. Wildfire: Damage to infrastructure and human operations.
   b. Power Outages: Disruption to user services.
   c. Network Disruption: Network instability that disrupts communication between applications, APIs, and payment gateways.

2. Human: Human activities that may interrupt or harm the system.
   a. Operator Error: Errors in data entry or system configuration, such as providing an inaccurate shipping address.
   b. Cyber Attack: Fraudulent attempts to gain access to user or administrative credentials.
   c. User Irresponsibility: Potential unauthorized access to user accounts and personal data.
3. Virus: Malicious software that may interrupt or harm the system.
   a. Malware: Malicious software that can infect servers, applications, and computers.
   b. Ransomware: A virus that encrypts data and demands a ransom to regain access.

Vulnerability Identify

During this phase, several vulnerabilities may risk the system of STNKGO. After analyzing the system, here are some vulnerabilities in the system.

Table 7. Vulnerability Identification

Threat Code	Asset Code	Vulnerability	Vulnerability Code
TE1	H1, H2	There is a lack of data redundancy and secure backup server locations.	V1
TE2	H1, H2	There are no backup power sources, such as a UPS or power generator.	V2
TE3	S1-S6	There is either no network failover or an unreliable network connection.	V3
TH1	D1-D5	Lack of training or SOP for operators in managing data.	V4
TH2	D1-D5, S1-S6	lack of two-factor authentication or other safeguards against unauthorized access.	V5
TH3	HR1-HR4	Lack of knowledge by users about security procedures, including using weak passwords.	V6
TV1	S1-S6	The computer lacks antivirus software or does not update its software regularly.	V7
TV2	D1-D5	Data is not regularly and securely backed up, or it is not encrypted.	V8

STNKGO's employees have made several updates to control each vulnerability and improve the apps themselves. The control that has been made by employees can be seen in the following table.

Table 8. Control Analysis

Threat Code	Asset Code	Vulnerability Code	Control
TE1	H1, H2	V1	Use a cloud service provider with multiple server locations
TE2	H1, H2	V2	Use a data center with backup power sources such as generators.
TE3	S1-S6	V3	Use redundant internet connections, and implement an automatic failover system for the primary network.
TH1	D1-D5	V4	Create clear SOPs for data management and conduct regular training for operators.

TH2	D1-D5, S1-S6	V5	Implement two-factor authentication for all access, and use firewalls and IDS/IPS to prevent attacks.
TH3	HR1-HR4	V6	Educate users about the importance of strong passwords, and enforce complex password policies.
TV1	S1-S6	V7	Create procedures for installing antivirus and regularly update the software.
TV2	D1-D5	V8	Encrypt sensitive data and create backup data regularly.

Vulnerability Identify

At this step, the likelihood of a threat event existing and the potential for threats to have adverse impacts are used to calculate the overall probability level of threat occurrence for each vulnerability. Tables 1 and 2 indicate the scale of this likelihood determination assessment. Table 9 shows the results of each vulnerability's total potential threat level to STNKGO's IT assets.

Table 9. Determination of Likelihood

Threat	Asset	Vulnerability	Likelihood Threat	Likelihood Threats That Have	Overall
TE1	H1, H2	V1	Low	High	Moderate
TE2	H1, H2	V2	Moderate	Moderate	Moderate
TE3	S1-S6	V3	Moderate	High	High
TH1	D1-D5	V4	Moderate	Moderate	Moderate
TH2	D1-D5,	V5	High	High	High
TH3	HR1-HR4	V6	Moderate	Moderate	Moderate
TV1	S1-S6	V7	High	High	High
TV2	D1-D5	V8	High	High	High

Determination of Impact

At that point, if the danger appears at STNKGO, an analysis of the effects of threats from each vulnerability occurs. The level of effect will then be decided by taking into consideration the possible impact that could be caused. Table 3 displays the assessment scale used to gauge the degree of effect. Table 10 displays the results of the examination of the threat impact and impact levels of every vulnerability related to STNKGO's IT assets.

Table 10. Determination of Impact Level

Threat Code	Asset Code	Vulnerability Code	Impact	Impact Level
TE1	H1, H2	V1	Financial losses, operational disruptions, and the loss of physical infrastructure	High
TE2	H1, H2	V2	Operational delays and interruptions in service access	Moderate

TE3	S1-S6	V3	User's inability to access the system and the possibility of data loss during transactions	High
TH1	D1-D5	V4	Data is incorrectly input or lost due to operator error	Moderate
TH2	D1-D5, S1-S6	V5	Risk of serious financial losses, application outages, and sensitive data theft	High
TH3	HR1-HR4	V6	Security-threatening flaws in data management or authentication	Moderate
TV1	S1-S6	V7	Data loss, system failure, and service disruptions	High
TV2	D1-D5	V8	Financial effects of ransom demands, loss of access, and encrypted data	High

The process of calculating the possible influence or effects of a threat materializing is known as "impact level determination." The impact levels are divided into three categories (Moderate, High, and Very High) based on the table that is shown. This is a comprehensive explanation:

1. Very High Impact:
   a. Cyberattacks: Cause system outages, negative publicity, the theft and leakage of private information, and large financial losses.
   b. Ransomware: Disrupts operations and finances by encrypting data, preventing access to vital systems, and possibly requiring ransom payments.
   c. Malware: Degrades system integrity significantly by causing service interruptions, system failures, and data corruption.
2. High Impact:
   a. Wildfires: Cause physical destruction to hardware, including operator PCs and cloud servers, which can lead to lost revenue and operational downtime.
   b. Network disruptions: Make it difficult for administrators and users to access necessary services, which can lead to delays in workflow and possibly erode trust.
   c. Unauthorized Access: Causes sensitive user or corporate data to leak and compromises system credentials.
3. Moderate Impact:
   a. Power outages: Damage hardware and server performance, causing service delivery delays and short-term operational difficulties.
   b. Operator errors can result in missing or inaccurate data entry, which can cause operational inefficiencies and small financial losses.
   c. User irresponsibility raises the possibility of security breaches by resulting in inadequate authentication procedures or improper credential handling.

The basis on which to determine the total level of risk is this impact level determination along with the probability of these occurrences. It is essential for creating successful IT risk management plans that reduce vulnerabilities and safeguard company resources.

Risk Determination

At this stage, each vulnerability's threat risk level is established using the overall likelihood and impact levels established in the preceding step. Table 4 displays the risk determination evaluation scale. Table 11 shows the results for each vulnerability's danger risk level.

Table 11. Risk Determination

Threat Code	Asset Code	Vulnerability Code	Overall Likelihood	Impact Level	Overall Risk
TE1	H1, H2	V1	Moderate	High	High
TE2	H1, H2	V2	Moderate	Moderate	Moderate
TE3	S1-S6	V3	High	Moderate	High
TH1	D1-D5	V4	Moderate	Moderate	Moderate
TH2	D1-D5, S1-S6	V5	High	High	High
TH3	HR1-HR4	V6	Moderate	Moderate	Moderate
TV1	S1-S6	V7	High	High	Very High
TV2	D1-D5	V8	High	High	Very High

According to Table 11. Risk Determination, cyberthreats (ransomware, trojans, and cyberattacks) pose the greatest risk due to their extremely high likelihood and impact. The possibility of malware and network interruptions, both of which have a high probability and impact, come next. High risks also include hazards associated with human factors, such as operator error and unauthorized access. On the other hand, viruses and natural disasters (wildfires and power outages) pose a considerable risk, while user carelessness and low power outages pose the least risk.

To minimize the threat risk of each of these vulnerabilities, STNKGO can mitigate risk by adding control measures to each threat. Control recommendations that can be used by STNKGO in minimizing the threat of any vulnerability that can threaten the IT assets owned by STNKGO can be seen in Table 12.

Control Recommendations

Table 12. Control Recommendations

Threat Code	Asset Code	Vulnerability Code	Control Recommendations
TE1	H1, H2	V1	Data centers should have fire suppression systems installed, and put backup and disaster recovery plans into action.
TE2	H1, H2	V2	To avoid downtime, install UPS (Uninterruptible Power Supply) systems. Make use of backup generators and redundant power sources.
TE3	S1-S6	V3	Implement network monitoring tools for early detection. For optimal network reliability, use a content delivery network (CDN). Establish redundant network paths and load balancing.
TH1	D1-D5	V4	To prevent data entering errors, regularly instruct users. Put data entry review procedures and validation checks into action.
TH2	D1-D5, S1-S6	V5	For all essential functions, use multi-factor authentication (MFA). Use the least privilege concept to guide the implementation of access control measures. Implement security audits frequently.
TH3	HR1-HR4	V6	All staff ought to attend security awareness training. Limit unwanted data access by using role-based access constraints.
TV1	S1-S6	V7	Update antivirus program frequently, and use endpoint security. To find malware, run security scans regularly. Make use of intrusion detection/prevention systems (IDS/IPS) and firewalls.

TV2	D1-D5	V8	For sensitive data, implement endpoint encryption. To stop unwanted data transmission, use data loss prevention (DLP) approaches. To recover encrypted data, ensure that backup and recovery procedures are in place.

CONCLUSION

The increasing reliance on digital platforms for public services, such as the STNKGO application for payment and delivery of Vehicle Registration Certificates, necessitates a robust and structured approach to information technology risk management. This study has highlighted the importance of implementing the NIST SP 800-30 Revision 1 framework to systematically identify, assess, and mitigate potential risks within the STNKGO system. The adoption of this framework enables a comprehensive understanding of the threats, vulnerabilities, and impacts associated with the application's core assets, including user data, payment systems, and service delivery processes. Through the application of the NIST framework, STNKGO can effectively map and categorize its IT assets and assess the likelihood and severity of risks such as cyberattacks, data breaches, unauthorized access, and transaction fraud. These risks are particularly critical given the sensitivity of the data processed—ranging from personal identity information to financial details. By conducting structured risk assessments and prioritizing risks based on their potential impact, the organization is better positioned to deploy targeted mitigation strategies that reduce exposure and strengthen system resilience.

The findings from this study emphasize that cybersecurity must be a central focus in the development and ongoing operation of the STNKGO platform. This involves not only the implementation of technical controls, such as encryption, secure authentication, and access restrictions, but also the institutionalization of organizational practices that promote awareness and accountability among employees. Standardized protocols, continuous staff training, and clear cybersecurity policies are essential to reducing the human factor in risk exposure. Moreover, the proactive application of the NIST SP 800-30 Revision 1 framework supports the organization's broader goals of maintaining public trust, complying with data protection regulations (such as the PDP Act), and ensuring uninterrupted service delivery. By identifying weaknesses before they are exploited and applying layered defenses, STNKGO can significantly reduce the likelihood of system downtime or reputational damage due to security incidents.

Another key takeaway from this study is the importance of continuous risk monitoring. IT risk management is not a one-time task but a dynamic process that must evolve alongside emerging threats and changes in the technological landscape. Regular updates to the risk assessment, along with periodic reviews of mitigation measures, will ensure that STNKGO remains adaptable and resilient in the face of evolving challenges. In conclusion, by leveraging the structured methodologies provided by the NIST SP 800-30 Revision 1 framework, STNKGO can enhance its information security posture, safeguard critical IT infrastructure, and ensure business continuity. This approach not only mitigates existing vulnerabilities but also establishes a culture of security awareness and continuous improvement—both of which are vital for sustaining trust and operational excellence in the digital delivery of public services.

REFERENCES

[1] Marbun, N. W., Iz, F. A., Ramadhan, M., Kogoya, L. J. H., Nugraha, L. F., & Nugraha, U. (2024). Payment and Transaction Risk Management at Coffeeshop X Using NIST 800-30 Framework. *JUSTINFO | Jurnal Sistem Informasi Dan Teknologi Informasi*, *1*(2), 135–146. https://doi.org/10.33197/justinfo.vol1.iss2.2023.1745

[2] Septiawan, M. A., Dermawan, A., Nur, A., Phasya, A., Adipermana, A. A., & Nugraha, U. (2024). Risk Management of Outdoor Equipment Rental Information System Using NIST SP 800-30 Framework at PT. XYZ. *Sistem Informasi Dan Teknologi Informasi*, *2*(1). https://doi.org/10.33197/justinfo.v2i1.1743

[3] Ahlul, Aziz., Sri, Wulandari. (2024). Advancing Business Services Through Web and Mobile Application Development. Jurnal Electric Electronic Communication Control Information System, doi: 10.21776/jeeccis.v17i3.1657

[4] Sergio, Sánchez-Fernández., E., Lasa., S., Terrados., Francisco, Javier, Sola-Martínez., Sara, Martínez-Molina., Marta, López, de, Calle., Paula, Cabrera-Freitag., María, José, Goikoetxea. (2023). Mobile/web application for monitoring food oral immunotherapy in children (Preprint). doi: 10.2196/preprints.54163

[5] Avner, Aronov. (2023). Development of mobile and web applications in the context of ukraine's digital transformation on the example of diia. Telekomunìkacìjnì ta ìnformacìjnì tehnologìï, 81(4) doi: 10.31673/2412-4338.2023.041213

[6] Abdul, Razak, Rahmat., Jasmin, Mohamed, Jamil., Baharudin, Osman., Shukree, bin, Osman. (2024). Commercialised durian plantation: development and design of web and mobile application. doi: 10.32890/jdsd2024.2.1.7

[7] Alma, Iftina, Azzahra, Ain., Awalludiyah, Ambarwati., Lukman, Junaedi. (2022). Analisis Manajemen Risiko Teknologi Informasi dan Keamanan Aset Dengan Menggunakan Nist Sp 800-30 Revisi 1. Jurnal Ilmu Komputer dan Bisnis, 13(2a):155-165. doi: 10.47927/jikb.v13i2a.403

[8] Benfano, Soewito. (2023). Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector. International Journal of Advanced Computer Science and Applications, 14(4) doi: 10.14569/ijacsa.2023.0140468

[9] Sindi, Aprianti., Renny, Puspita, Sari., Ibnur, Rusi. (2023). Manajemen Risiko Keamanan Simbada Menggunakan Metode NIST SP 800-30 Revisi 1 dan Kontrol ISO/IEC 27001:2013. Jurnal Buana Informatika, doi: 10.24002/jbi.v14i01.7043

[10] Megawati, Megawati., Siti, Rosnawati. (2022). Penilaian risiko jaringan komputer menggunakan framework nist sp 800-30 revisi 1 pada smk muhmmadiyah 2 pekanbaru. Jurnal ilmiah rekayasa dan manajemen sistem informasi, 8(2):189-189. doi: 10.24014/rmsi.v8i2.19115