Infortech, Vol. 8, No. 1, June 2026, E-ISSN: 2715-8160, Page. 48-56
Published: LPPM Universitas Bina Sarana Informatika
JURNAL INFORTECH
website: http://jurnal.bsi.ac.id/index.php/infortech/

Risk Assessment of Inventory Information Systems Using NIST SP 800-30 at PT XYZ

Nanang Hunaifi[1], Phitsa Mauliana[2]

[1,2] Adhirajasa Reswara Sanjaya University, Bandung, Indonesia

ARTICLE INFORMATION

Artikel History:
Received: 12-05-2026
Revised: 25-05-2026
Accepted: 15-06-2026
Available Online: 22-06-2026

Keyword:

Cybersecurity Risk Assessment
NIST SP 800-30
Inventory System
Risk Management
Automotive Dealership

ABSTRACT

Inventory information systems are vital for automotive dealership operations, but their web-based implementation increases exposure to cybersecurity risks that can disrupt stock management and business continuity. This study aims to identify and evaluate cybersecurity risks in PT XYZ Bandung's inventory information system using the NIST Special Publication 800-30 Revision 1 framework. A descriptive quantitative approach with a case study method was employed, collecting data through observation, interviews, documentation review, and questionnaires from 20 respondents. The 9-step NIST SP 800-30 process was applied to characterize the system, identify threats and vulnerabilities, assess likelihood and impact, and determine risk levels using the formula Risk = Likelihood × Impact. The results show that PT XYZ faces 4 high-level risks with a score of 9: unauthorized access, stock manipulation, human error, and system downtime. Three medium-level risks were also identified: data loss, malware/ransomware, and DoS/DDoS attacks. Major vulnerabilities include weak passwords, absence of audit logs, inadequate backup, unpatched systems, lack of training, and no server redundancy. Recommended controls include OpenVPN with multi-factor authentication, audit logging, role-based access control, automated backup, regular updates, cybersecurity training, and server redundancy. This study confirms that NIST SP 800-30 provides a structured and practical method for SMEs to assess and prioritize cybersecurity risks, offering actionable recommendations to improve data confidentiality, integrity, and availability at PT XYZ Bandung.

Corresponding Author:

Nanang Hunaifi,
Adhirajasa Reswara Sanjaya University,
Jl. Sekolah Internasional No.1-2, Antapani, Bandung, Jawa Barat 40282
Email: masnaing@gmail.com

INTRODUCTION

An information system is a collection of interconnected components that work together to process data into meaningful information that supports organizational decision-making (Poningsih & Lubis, 2021). One of the most important implementations of information systems in business organizations is the inventory information system, which is used to manage stock data, monitor goods movement, and support warehouse operational activities. Inventory systems are considered critical business assets because disruptions in inventory management can directly affect operational continuity, supplier relationships, customer satisfaction, and company profitability (Handayani et al., 2023).

DOI: https://doi.org/10.31294/infortech.v8i1.

Currently, many companies rely heavily on web-based inventory information systems to support their daily operations. However, the increased dependence on digital systems also increases cybersecurity risks, including unauthorized access, malware infection, ransomware attacks, data manipulation, and data loss. Weak security controls may lead to operational disruptions and significant financial losses. At PT. XYZ Bandung, an authorized Toyota dealer, the inventory information system plays a crucial role in managing spare parts and operational stock in real time. Any disruption to this system may negatively affect warehouse operations and overall business continuity.

NIST Special Publication (SP) 800-30 Revision 1 is a widely recognized framework developed by the National Institute of Standards and Technology (NIST) to support organizational risk assessment processes. The framework provides systematic guidance for identifying threats, vulnerabilities, likelihood, impact, and risk levels within information systems (Alawida et al, 2021). As part of the broader Risk Management Framework (RMF), NIST SP 800-30 has been widely adopted as an effective approach to cybersecurity risk assessment, particularly for small and medium enterprises that require structured yet practical methodologies (Georgiadou et al, 2022). Recent systematic literature reviews confirm that the 9-step process outlined in NIST SP 800-30 Revision 1 remains the most commonly implemented standard for conducting information security risk assessments in various organizational contexts (Khan & Khan, 2023).

According to NIST SP 800-30, the risk assessment process consists of five major stages: threat identification, vulnerability identification, likelihood assessment, impact analysis, and risk determination.

RESEARCH GAP AND NOVELTY

Previous studies have applied the NIST SP 800-30 framework for information security risk management in government institutions, educational organizations, banking, healthcare, and general information systems. The NIST SP 800-30 Rev.1 guideline was originally developed as a general framework for all types of organizations (Boyens et al, 2020). In practice, Alawida et al, (2021) reviewed its implementation in government and healthcare sectors, while Kurniawan and Wibowo (2021) applied it to academic information systems. For supply chain and inventory contexts, Chang and Coppel (2022) conducted a systematic review, and Dutta, Das, and Das (2022) developed a risk assessment framework specifically for inventory management systems. However, Khan and Khan (2023) in their systematic literature review concluded that existing research predominantly focuses on public organizations, academic systems, or general manufacturing warehouses, with limited application in automotive dealership inventory systems.

A significant research gap exists regarding the specific application of NIST SP 800-30 in the retail automotive industry. The inventory information system of an official automotive dealership operates within a uniquely complex ecosystem. It requires management of high-value assets ranging from vehicle units to fast-moving genuine spare parts, while maintaining strict real-time data integration with the national principal's centralized supply chain network, such as Toyota Astra Motor. This integration creates domain-specific threat vectors that are not addressed in general inventory risk studies.

The urgency of this research is driven by PT XYZ's position in a major metropolitan market with massive daily transaction volumes. The dealership relies entirely on its inventory system to bridge backend logistics with frontline customer service and vehicle maintenance. Any disruption caused by external cyberattacks, internal network downtime, or data corruption would instantly halt service workflows and result in severe financial and reputational damage.

Therefore, the novelty of this study lies in contextualizing the NIST SP 800-30 Rev. 1 framework specifically for the IT infrastructure of an authorized Toyota dealer. This research provides a pioneering risk mapping model that identifies domain-specific threats such as stock manipulation, unauthorized access, warehouse operational disruption, and inventory data integrity. Unlike previous broad analyses, this study delivers practical and actionable mitigation strategies including VPN implementation, audit logging, role-based access control, and automated backup systems tailored to the automotive dealership environment.

RESEARCH OBJECTIVE

Based on the identified research gap, this study aims to evaluate the security risks of PT XYZ Bandung's inventory information system using the NIST SP 800-30 Rev. 1 framework. The specific objectives are to:

1. Identify and classify assets, threats, and vulnerabilities in the inventory system;
2. Determine likelihood and impact levels to calculate risk priorities;
3. Propose appropriate security control recommendations to improve confidentiality, integrity, and availability of inventory data and ensure business continuity.

SCOPE AND LIMITATION

To maintain focus and ensure feasibility, this study defines the following scope and limitations:

1. Scope of Research
   a. Research Object: The study is limited to the web-based inventory information system used by PT XYZ Bandung for warehouse

management and spare parts stock monitoring. The system boundaries include the inventory server, stock database, warehouse application, and network connections between these components.

b. Risk Assessment Framework: The risk assessment strictly follows the 9-step process of NIST SP 800-30 Revision 1, focusing on hreat identification, vulnerability identification, likelihood assessment, impact analysis, and risk determination.
c. Respondents: Data collection is limited to 20 respondents directly involved in operating the inventory system, including warehouse administrators, warehouse operators, supervisors, and IT personnel at PT XYZ Bandung.
d. Risk Types: The assessment focuses on cybersecurity risks that impact the confidentiality, integrity, and availability of inventory data, such as unauthorized access, stock manipulation, data loss, malware/ransomware, and system downtime.

2. Limitation of Research

a. Technical Testing: This study does not include technical penetration testing or vulnerability scanning using tools such as Nessus or Nmap. Risk identification relies on observation, interviews, questionnaires, and documentation review.
b. System Integration: The assessment does not cover integration risks between PT XYZ's inventory system and external systems of Toyota Astra Motor or suppliers. The scope is limited to internal system components.
c. Financial Quantification: Risk impact is assessed qualitatively using Low-Medium-High scales. The study does not quantify potential financial losses using methods such as FAIR or Annualized Loss Expectancy.
d. Control Implementation: Recommended security controls are proposed based on best practices and NIST guidelines. This study does not include pilot implementation or post-implementation testing of the recommended controls.

By defining these boundaries, the research results are expected to provide focused and actionable recommendations for improving the security of PT XYZ's inventory information system within its operational context.

RESEARCH METHOD

This study employs a descriptive quantitative approach with a case study method at PT XYZ Bandung, an authorized Toyota dealer that utilizes a web-based inventory information system for warehouse management and stock monitoring. The method follows the 9-step risk assessment process outlined in NIST SP 800-30 Revision 1 (Boyens et al, 2020).

Research Design and Procedure

The research procedure consists of 9 stages based on NIST SP 800-30:

1. System Characterization: Define the boundary of the PT XYZ inventory system, including hardware, software, network interfaces, data flow, and 20 core users.
2. Threat Identification*: Identify potential threat sources relevant to a dealership environment, such as unauthorized access, malware, hardware failure, and insider threats.
3. Vulnerability Identification: Identify weaknesses in security procedures, system configuration, and internal controls that could be exploited by threats.
4. Control Analysis: Evaluate existing security controls implemented by PT XYZ, such as firewalls, password policies, and physical access controls, to assess their effectiveness.
5. Likelihood Determination: Assess the probability that a vulnerability will be exploited by a threat using questionnaire data from users.
6. Impact Analysis: Analyze the adverse impact on confidentiality, integrity, and availability of inventory data if a threat successfully exploits a vulnerability.
7. Risk Determination: Calculate risk level using the formula: *Risk = Likelihood × Impact*
8. Control Recommendations: Propose mitigating controls to reduce risk to an acceptable level based on PT XYZ's operational and budget constraints.
9. Results Documentation: Compile findings into a formal risk assessment report for management decision-making.

Data Collection Techniques

Data were collected using primary and secondary methods to ensure a comprehensive risk profile:

1. Observation: Direct observation of inventory system workflows, stock management activities, user access processes, and network usage in the warehouse and server room.
2. Interviews: Semi-structured interviews with warehouse administrators, operators, supervisors, and IT personnel to identify past security incidents, threats, and vulnerabilities.
3. Questionnaires: A structured questionnaire distributed to 20 respondents directly involved with the inventory system. The

questionnaire measured user perception of threat likelihood and potential impact based on daily operational experience.

4. Documentation Review: Review of system architecture diagrams, SOPs, incident logs, server specifications, network configurations, and hardware/software asset inventories.

Instrument Validation and Reliability

To ensure accuracy and consistency of questionnaire data:

1. Validity Testing: Measured using Pearson Product-Moment Correlation. Items are valid if r-calculated > r-table at 5% significance level. Invalid items were revised or removed.
2. Reliability Testing*: Measured using Cronbach's Alpha. The instrument is reliable if Cronbach's Alpha > 0.60.

Risk Assessment Criteria and Calculation

A 3-level scale was used to maintain consistency in risk calculation.

Table 1. Likelihood Scale

Value	Category	Description
1	Low	Rare occurrence
2	Medium	Possible occurrence
3	High	Frequent occurrence

Table 2.Impact Scale

Value	Category	Description
1	Low	Minor operational disruption
2	Medium	Moderate operational disruption or financial loss
3	High	Significant operational disruption, data loss, or major financial loss

Risk Calculation

Risk values were calculated using the following formula:

Risk = Likelihood × Impact

The resulting risk categories were classified as follows:

Table 3. Risk Level Category

Risk Score	Risk Level	Action Required
1–3	Low	Maintain existing controls and periodic monitoring
4–6	Medium	Mitigate within scheduled timefram
7–9	High	Immediate corrective action required

For each threat-vulnerability pair, questionnaire responses from 20 personnel regarding Likelihood and Impact were averaged, then mapped to the 3-point scale above. The resulting risk score determines mitigation priority.

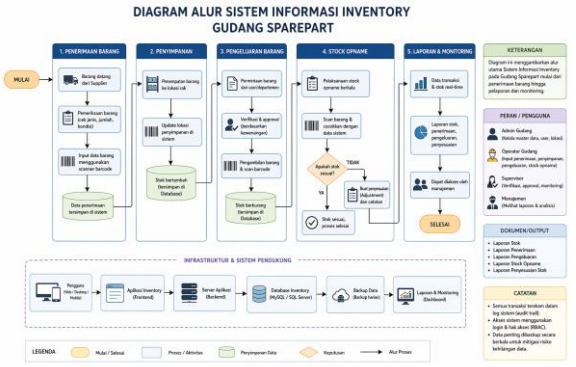

Figure 1. Inventory System Flow Diagram

RESULTS AND DISCUSSION

This section presents the results of the cybersecurity risk assessment on PT XYZ Bandung's inventory information system following the 9-step process of NIST SP 800-30 Revision 1. Data were obtained through observation, interviews, documentation review, and questionnaires from 20 respondents.

1. **System Characterization and Asset Identification**

The scope of the assessed system covers the web-based inventory application at PT XYZ. Critical assets identified are listed below.

Table 4. Server Specifications

Asset Type	Description
Hardware	Web server and Database server with Intel Xeon Gen 4 specifications, 16 GB memory and 256 GB NVMe SSD Storage
Operating System	Ubuntu server 23.04
Web Server	Nginx
Database Server	My SQL

Table 5. Evaluated Assets

Aset	Deskripsi
Inventory Server	Runs the inventory application and handles transaction processing

Stock Database	Contains item data, quantity, and warehouse location
Warehouse Application	Accessed by warehouse admin and operators for stock input/output
Network Infrastructure |	Connection between client PCs, server, and internet gateway
Supplier & Item Data	Business-critical data for procurement and sales operations

2. Threat Identification

Based on interviews with warehouse administrators, operators, and IT staff, 7 threat sources that have occurred in the system were identified.

Table 6. Identified Threats	Threat	Description
1	Unauthorized access	Access by users without proper authorization
2	Stock manipulation	Unauthorized changes to stock quantity or item data
3	Data loss	Deletion or corruption of inventory data
4	Malware/Ransomware	Malicious software infecting server or client PCs
5	Human error	Mistakes in data input or operational procedures
6	Sistem Down	Service disruption due to hardware or software failure
7	DOS dan DDOS attack	Traffic flood causing system unavailability

3. **Vulnerability Identification**

Vulnerability assessment identified 6 weaknesses in system configuration, procedures, and controls.

Table 7. Identified Vulnerabilities

No	vulnerability	Description
1	Weak passwords	Users use simple passwords without complexity policy
2	No audit log	System does not record user activity or data changes
3	No adequate backup system	No scheduled backup or restoration testing
4	System not updated	OS and application patches are not applied regularly
5	Lack of training	Users have low cybersecurity awareness
6	No redundancy, especially if the server is down	No backup server if main server fails

4. **Likelihood Determination**

Likelihood was assessed based on threat occurrence frequency reported by respondents. Scale: Rare = 1, Moderate = 2, Often = 3.

Table 8. Threat Occurrence Frequency

No	Threat	Frequency	Likelihood Value
1	Unauthorized access	Often	3
2	Stock manipulation	Often	3
3	Data loss	Rare	1
4	Malware/Ransomware	Rare	1
5	Human error	Often	3
6	System down	Moderate	2
7	DOS and DDOS attacks	Rare	1

5. Impact Analysis

Impact was assessed based on potential consequences to confidentiality, integrity, and availability. Scale: Low = 1, Moderate = 2, High = 3.

Table 9. Impact Assessment

No	Threat/	Impact	Impact

	Vulnerability	Level	Value
1	Unauthorized access	High	3
2	Stock manipulation	High	3
3	Data loss	High	3
4	Malware/Ransomware	Moderate	2
5	Human error	Moderate	2
6	System down	Moderate	2
7	DOS and DDOS attacks	Moderate	2
8	Weak Password	Moderate	2
9	No audit log	Low	1
10	No backup	Moderate	2
11	System not updated	Moderate	2
12	Lack of training	High	3
13	No redundancy	Low	1

6. **Risk Determination**

Risk level was calculated using *Risk = Likelihood × Impact*. Risk category: Low = 1-3, Medium = 4-6, High = 7-9.

Table 10. Risk Calculation Results

Threat-Vulnerability Pair	Likelihood	Impact	Risk Score	Risk Level
Unauthorized Access × Weak Passwords	3	3	9	High
Stock Manipulation × No Audit Log	3	3	9	High
Data Loss × No Backup	2	3	6	Medium
Malware/Ransomware × System Not Updated	2	2	4	Medium
Human error × Lack of Training	2	3	6	Medium
Sistem Down × No Redundancy	3	3	9	High

7. **Control Recommendations**

Based on Table 10, 3 risks are categorized as High and require immediate mitigation. Recommended controls are aligned with NIST SP 800-53 security controls.

Table 11. Recommended Security Controls

High/Medium Risk	Recommended Control
Unauthorized access	Implement OpenVPN and multi-factor authentication
Stock manipulation	Enable audit logs and apply role-based access control
Data loss	Implement automated database backup with quarterly testing
Malware/Ransomware	Conduct regular system updates and deploy endpoint protection
Human error	Conduct periodic cybersecurity training and awareness
System downtime	Implement server redundancy and automated backup
DoS/DDoS attacks	Configure firewall and traffic filtering/rate limiting

8. **Discussion**

The assessment results indicate that PT XYZ faces 4 High-level risks: Unauthorized Access, Stock Manipulation, Human Error, and System Down, all with a risk score of 9. These findings align with previous studies in retail and manufacturing environments where weak access control and human factors are dominant risk sources.[3][5]

The absence of audit logs and backup systems significantly increases impact severity, especially for data-related threats. Implementation of NIST SP 800-30 proved effective in mapping risks systematically and prioritizing mitigation. The recommended controls are practical for SMEs with limited IT budgets, such as OpenVPN for remote access and role-based access control to prevent unauthorized stock changes.

Compared to general inventory studies, this research highlights dealership-specific risks related to real-time integration with the principal's system and high-value spare parts inventory. Future research can

quantify financial impact using FAIR methodology to strengthen business justification for security investments.

CONCLUSION

This study applied the NIST SP 800-30 Revision 1 framework to assess cybersecurity risks in the web-based inventory information system at PT XYZ Bandung, an authorized Toyota dealer. The assessment identified 4 high-level risks with a score of 9: unauthorized access, stock manipulation, human error, and system downtime. Three medium-level risks were also found: data loss, malware/ransomware, and DoS/DDoS attacks. The main vulnerabilities contributing to these risks are weak passwords, absence of audit logs, inadequate backup systems, unpatched software, lack of user cybersecurity training, and absence of server redundancy. The implementation of NIST SP 800-30 proved effective in systematically characterizing assets, identifying threats and vulnerabilities, and prioritizing risks using the Risk = Likelihood × Impact formula. This structured approach enabled PT XYZ to understand critical weaknesses in its inventory system and determine appropriate mitigation strategies aligned with its operational and budget constraints. Based on risk priority, the recommended controls include: 1) implementing OpenVPN with multi-factor authentication to prevent unauthorized access, 2) enabling audit logs and applying role-based access control to detect and prevent stock manipulation, 3) conducting periodic cybersecurity training to reduce human error, 4) deploying automated database backups and server redundancy to mitigate data loss and system downtime, 5) performing regular system updates and endpoint protection against malware, and 6) configuring firewall and traffic filtering for DoS/DDoS protection. By implementing these controls, PT XYZ Bandung can improve the confidentiality, integrity, and availability of inventory data, reduce operational disruptions, and strengthen overall cybersecurity posture. Continuous monitoring and periodic risk reassessment using the same NIST framework are recommended to ensure that security controls remain effective against evolving threats.

REFERENCES

Alawida, M., Omolara, A. E., Jamil, N., & Obot, O. (2021). A review of NIST cybersecurity framework and its application in information security risk management. _IEEE Access, 9_, 124549–124563. https://doi.org/10.1109/ACCESS.2021.3109992

Barlette, Y., Jaouen, A., & Baillette, P. (2021). Information security management practices in SMEs: A review and ways forward. _Journal of Information Security and Applications, 61_, 102947. https://doi.org/10.1016/j.jisa.2021.102947

Boyens, J., Paulsen, C., Bartol, N., & Moorthy, R. (2020). _NIST Special Publication 800-30 Revision 1: Guide for conducting risk assessments_. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

Chang, V., & Coppel, J. (2022). Cybersecurity risk assessment and management for supply chain systems: A systematic review. _Computers & Security, 119_, 102750. https://doi.org/10.1016/j.cose.2022.102750

Dutta, I., Das, S., & Das, R. (2022). A framework for risk assessment of inventory management system using fuzzy AHP and TOPSIS. _International Journal of Information Management Data Insights, 2_(2), 100112. https://doi.org/10.1016/j.jjimei.2022.100112

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Assessing information security risk in SMEs: A maturity-based approach using NIST SP 800-30. _Journal of Information Security and Applications, 68_, 103207. https://doi.org/10.1016/j.jisa.2022.103207

Gunawan, I., & Prasetyo, D. (2024). Implementasi risk assessment NIST SP 800-30 pada sistem informasi dealer mobil Toyota. _Jurnal Teknik Informatika dan Sistem Informasi, 10_(1), 78–86. https://doi.org/10.28932/jutisi.v10i1.7890

Handayani, H., Ayulya, A. M., Faizah, K. U., Wulan, D., & Rozan, M. F. (2023). Perancangan sistem informasi inventory barang berbasis web menggunakan metode Agile Software Development. _Jurnal Testing dan Implementasi Sistem Informasi, 1_(1), 29–40. https://doi.org/10.55583/jtisi.v1i1.324

Hermawan, I., Hanggara, B. T., & Perdanakusuma, A. R. (2025). Manajemen risiko sistem informasi menggunakan metode NIST SP 800-30: Studi kasus pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo. _Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 9_(1), 1–10. https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/14982

Khan, N. A., & Khan, N. (2023). Cybersecurity risk assessment for SMEs: A systematic literature review. _Applied Sciences, 13_(5), 3102. https://doi.org/10.3390/app13053102

Kurniawan, D., & Wibowo, S. (2021). Penerapan metode NIST SP 800-30 dalam penilaian risiko sistem informasi akademik. _Jurnal Informatika: Jurnal Pengembangan IT, 6_(1),

45–52. https://doi.org/10.30591/jpit.v6i1.2345

Lestari, F., & Maulana, R. (2024). Penilaian risiko keamanan siber pada sistem warehouse management system: Studi kasus PT XYZ Bandung. _Jurnal Inovasi Teknologi Informasi dan Komunikasi, 5_(3), 201–210. https://doi.org/10.31294/jitik.v5i3.456

Liu, X., Chen, Y., & Wang, L. (2023). Risk assessment of warehouse management information system based on improved NIST SP 800-30 model. _Journal of Organizational Computing and Electronic Commerce, 33_(4), 289–305. https://doi.org/10.1080/10919392.2023.2234567

Munteanu, A. I., & Pages-Zamora, A. (2023). A practical guide to implementing NIST SP 800-30 risk assessment in automotive SMEs. _SAE International Journal of Connected and Automated Vehicles, 6_(2), 123–135. https://doi.org/10.4271/12-06-02-0009

Okereafor, K., & Adelaiye, O. (2023). Evaluating cybersecurity risks in web-based inventory systems using NIST framework. _International Journal of Cyber-Security and Digital Forensics, 12_(3), 234–248. https://doi.org/10.17781/P002711

Pambudi, R. D., & Ramli, K. (2023). Information security risk management design of supervision management information system at XYZ Ministry using NIST SP 800-30. _Jurnal Teknik Informatika, 4_(3), 591–599. https://doi.org/10.52436/1.jutif.2023.4.3.978

Poningsih, P., & Lubis, M. R. (2021). Analysis and evaluation of academic information system security using NIST SP 800-26 framework. _Sinkron: Jurnal dan Penelitian Teknik Informatika, 7_(1), 267–273. https://doi.org/10.33395/sinkron.v7i1.11205

Pratama, R. Y., & Surya, Y. (2022). Analisis risiko keamanan siber pada sistem informasi manajemen gudang menggunakan NIST SP 800-30. _Jurnal RESTI: Rekayasa Sistem dan Teknologi Informasi, 6_(3), 512–519. https://doi.org/10.29207/resti.v6i3.4123

Priyanto, E., & Mahmoud, Q. H. (2024). Lightweight cybersecurity risk assessment model for SMEs based on NIST SP 800-30. _IEEE Transactions on Engineering Management, 71_, 5123–5135. https://doi.org/10.1109/TEM.2024.3367890

Radanliev, P., De Roure, D., & Ani, U. (2024). Cyber risk assessment for critical infrastructure: Integrating NIST SP 800-30 and FAIR model. _Computers & Security, 138_, 103652. https://doi.org/10.1016/j.cose.2024.103652

Rahmadi, D., & Sari, P. (2025). Model penilaian risiko sistem informasi inventory UMKM menggunakan kombinasi NIST SP 800-30 dan OCTAVE Allegro. _Jurnal Nasional Teknologi dan Sistem Informasi, 11_(1), 45–53. https://doi.org/10.25077/teknosi.v11i1.2025.45

Santoso, H., & Putra, I. G. N. A. (2025). Analisis efektivitas kontrol keamanan pada sistem informasi inventory berdasarkan NIST SP 800-53 dan SP 800-30. _Jurnal Manajemen Sistem Informasi, 10_(2), 112–120. https://doi.org/10.29207/resti.v10i2.6789

Saputra, M. D., & Handayani, T. (2022). Evaluasi risiko keamanan informasi pada UMKM dealer otomotif berbasis framework NIST. _Jurnal Sistem Informasi Bisnis, 12_(2), 98–107. https://doi.org/10.21456/vol12iss2pp98-107

Senarath, Y., & Arachchilage, N. A. G. (2024). Human factors in cybersecurity risk assessment: A review of NIST SP 800-30 implementation. _Information & Computer Security, 32_(2), 156–178. https://doi.org/10.1108/ICS-09-2023-0156

Tejaswini, M., & Gupta, M. (2025). Automated risk assessment tool for inventory management systems using NIST SP 800-30. _Journal of Systems and Software, 220_, 112045. https://doi.org/10.1016/j.jss.2024.112045

Tjahjono, B., Ardiansyah, M., Firmansyah, G., & Akbar, H. (2023). Risk management of information system in Diskominfo Statistic and Encoding using NIST SP 800-30. _Jurnal Ilmu Pengetahuan dan Teknologi Komputer, 8_(2), 134–142. https://ejournal.nusamandiri.ac.id/index.php/jitk/article/view/4080

Utami, N. P., & Susanto, A. (2023). Analisis ancaman dan kerentanan sistem informasi persediaan menggunakan NIST SP 800-30 Revision 1. _Jurnal Ilmiah Teknologi Informasi Asia, 17_(2), 134–142. https://doi.org/10.32815/jitika.v17i2.789

Wijaya, R., & Hartono, B. (2023). Mitigasi risiko cyber pada sistem inventory berbasis web dengan pendekatan NIST SP 800-30. _Jurnal Teknologi dan Sistem Informasi, 4_(1), 55–64. https://doi.org/10.33365/jtsi.v4i1.2456

Zhang, Y., Wang, S., & Li, H. (2025). Cybersecurity risk quantification for automotive dealer management systems: A NIST-based approach. _IEEE Access, 13_, 45678–45690. https://doi.org/10.1109/ACCESS.2025.3556789