DOI: https://doi.org/10.33197/justinfo.v3i1.3212 ISSN: 3031-3449

Systematic Literature Review: Implementation of IT Risk Management Using the NIST Framework in Education

[1]Cika Alpi Nurpauji, [2]Fahmi Idris Susanto, [3]Muhammad Firas Hisyam, [4]Muhamad Azmi, [5]Ucu Nugraha
[1]Sistem Informasi, Universitas Widyatama, Bandung, Indonesia, cika.alpi@widyatama.ac.id
[2]Sistem Informasi, Universitas Widyatama, Bandung, Indonesia, fahmi.idris@widyatama.ac.id
[3]Sistem Informasi, Universitas Widyatama, Bandung, Indonesia, firas.hisyam@widyatama.ac.id
[4]Sistem Informasi, Universitas Widyatama, Bandung, Indonesia, muhamad.azmi@widyatama.ac.id
[5]Sistem Informasi, Universitas Widyatama, Bandung, Indonesia, ucu.nugraha@widyatama.ac.id

ABSTRACT

The rapid advancement of information technology (IT) has significantly transformed various industries, including education, through the implementation of information systems that streamline student admissions, pedagogy, and institutional administration. However, this digital evolution introduces critical data security risks. Effective IT risk management is therefore essential to safeguard sensitive data and prevent operational disruptions within educational institutions. One of the most prominent frameworks for this purpose is NIST Special Publication 800-30, which provides systematic guidance for identifying and assessing IT-related risks. The NIST framework assists educational institutions in identifying potential threats and vulnerabilities while establishing robust mitigation strategies. While the framework possesses immense potential to elevate IT risk awareness, its implementation in the education sector remains hindered by resource constraints, varying levels of IT literacy, and regulatory complexities. This research employs the Systematic Literature Review (SLR) method to analyze the implementation of the NIST framework in managing IT risks within the education sector. This methodology enables the identification and evaluation of relevant research findings regarding both the successes and challenges associated with the framework's adoption. Through a comprehensive literature analysis, this study offers strategic insights and recommendations to enhance the effectiveness of the NIST framework within technology-driven educational environments.

Keywords: IT Risk Management, NIST SP 800-30, Systematic Literature Review, Educational Technology, Cybersecurity.

Corresponding Author:

Cika Alpi Nurpauji
Sistem Informasi, Universitas Widyatama
Bandung, Indonesia
cika.alpi@widyatama.ac.id

INTRODUCTION

The evolution of information systems (IS) and information technology (IT) has progressed exponentially across diverse sectors. Today, technological integration is a cornerstone of industrial business processes. Similarly, the educational sector has embraced IT to streamline student admissions, pedagogical processes, and institutional administration [1]. From learning management systems (LMS) that facilitate seamless educator-student interaction to communication platforms that drive collaborative research, IT is pivotal in enhancing the efficiency and effectiveness of modern education [2]. However, this intensified reliance on digital systems introduces emerging challenges regarding data security. Consequently, robust IT risk management is now essential to safeguard sensitive information and ensure the operational sustainability of educational institutions.

A premier approach to managing these risks is the application of the NIST Special Publication series. Developed by the National Institute of Standards and Technology (NIST) [3], this framework

provides systematic guidance for conducting comprehensive risk assessments of information systems [4].

NIST assists organizations in identifying potential threats and vulnerabilities that could jeopardize business processes, enabling the design of resilient mitigation strategies. By adopting the NIST framework [5], educational institutions gain a clearer understanding of their risk profiles, allowing for proactive measures to enhance resilience against cyberattacks and other security breaches.

The significance of IT risk management in education extends beyond data protection; it is a critical factor in maintaining institutional reputation [6]. Security incidents, such as data breaches, result in substantial financial losses and erode public trust [7]. Educational institutions serve as repositories for sensitive data, including personally identifiable information (PII), academic records, and financial data [8]. The compromise of this information carries severe legal implications and impacts the wellbeing of students and staff alike.

The NIST implementation process involves several interrelated phases. Initially, institutions must conduct asset identification, encompassing hardware, software, student data, and network infrastructure [9]. This is followed by identifying threats and vulnerabilities, which may arise from external cyberattacks, human error, or systemic failures.

Once these factors are mapped, a risk assessment is conducted to determine the potential impact of each threat by analyzing its likelihood and consequence. These results inform the development of mitigation strategies [10], which include technical controls like firewalls and encryption, alongside more stringent cybersecurity policies.

Despite the comprehensiveness of the NIST framework, educational institutions often face significant barriers during implementation [10]. Resource constraints are a primary obstacle; small schools or universities with limited budgets often lack the specialized IT personnel or financial capital required for a full-scale NIST deployment [11]. Furthermore, a lack of cybersecurity awareness among faculty and students presents a behavioral challenge. Without an organizational culture of security, best practices are difficult to sustain. The decentralized and complex organizational structures typical of large academic institutions also hinder the consistent application of security policies [12].

Moreover, the rapid pace of technological change adds a layer of complexity. As new cyber threats emerge, institutions must continuously update their protocols to remain resilient [13], necessitating an ongoing commitment to staff training and professional development [3]. Regulatory compliance further complicates the landscape, as institutions must align NIST implementation with various local and national data protection laws [14].

Against this backdrop, the present study aims to analyze the implementation of the NIST framework in the education sector, specifically identifying the most frequently utilized versions of the framework and the primary challenges encountered during adoption. Through a Systematic Literature Review (SLR), this study provides valuable insights into IT risk management best practices and offers strategic recommendations to enhance the effectiveness of NIST within educational settings. Ultimately, a deeper understanding of NIST implementation will assist institutions in protecting digital assets while fostering a secure environment for teaching and learning.

METHODOLOGY

This study employs the Systematic Literature Review (SLR) methodology. An SLR is a rigorous research method utilized to identify, evaluate, and synthesize all available research evidence relevant to a specific research question [15]. This approach follows a series of structured stages, including the formulation of research questions, the execution of a comprehensive literature search, the establishment of clear inclusion and exclusion criteria, the analysis and synthesis of findings, and finally, the compilation of the report and formulation of conclusions [16], [17]. The following roadmap outlines the systematic steps undertaken in this study to ensure a transparent and reproducible review process.

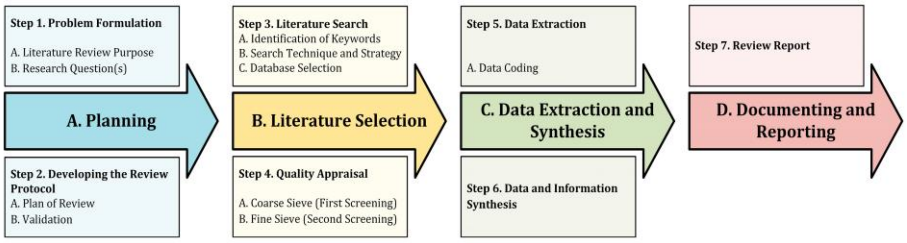

Figure 1. Roadmap Outlines The Systematic Literature Review (SLR) Methodology

Research Focus and Objectives

The initial phase of this study involved establishing a precise focus and strategic direction to ensure research alignment. The primary objective is to analyze the specific versions of the NIST Framework most frequently utilized for IT risk management in the educational sector, while simultaneously identifying the systemic challenges and barriers to their adoption. The selection of IT risk management as the central object of this research is motivated by the following critical factors:

1) The exponential growth and pervasive integration of information technology within educational institutions.
2) The emergence of high-level security risks and vulnerabilities inherently linked to the deployment of complex IT infrastructures in schools and universities.
3) The significant operational, financial, and reputational consequences that arise when IT risk management is inadequately executed within the academic environment.

Research Question Formulation

The subsequent phase involves the formulation of research questions (RQ) that are directly aligned with the core research topic. Establishing precise and relevant inquiries allows for the systematic identification of key search terms and ensures the selection of appropriate scholarly databases for literature acquisition. The development of these research questions is driven by the growing necessity and observable phenomena surrounding the implementation of the NIST Framework for IT risk management within the educational sector. By defining these questions, the study establishes a clear boundary for the review, ensuring that the synthesized findings directly address the critical gaps in current academic and professional discourse..

Table 1. Research Question

Code	Research Question
RQ1	How can the NIST Framework be effectively implemented to identify and mitigate IT risks in educational institutions in the digital age?
RQ2	What are the main challenges facing educational institutions in implementing the NIST Framework?

Literature Search and Identification

The literature search was executed through a systematic query of multiple electronic databases using predefined keywords and search strings. Primary data sources included Google Scholar and Semantic Scholar, chosen for their comprehensive coverage of both peer-reviewed journals and institutional reports. To ensure the identification of relevant studies, the following search strings were utilized:

1) "NIST IT Risk Management" "Education Industry"
2) "NIST IT Risk Management in Education" These keywords were systematically applied across each electronic database to capture literature at the intersection of cybersecurity frameworks and educational administration. Following the initial retrieval, relevant articles were screened and selected for detailed qualitative and quantitative analysis. Within the scope of this review, the most contemporary publications have been categorized as "New Studies" to highlight recent advancements and evolving trends in the field.

Article Selection and Screening

The articles identified in the previous stage were subjected to a rigorous screening process based on predefined selection criteria. To maintain contemporary relevance, the literature search was limited to studies published from 2019 onward. The evaluation process commenced with a preliminary

screening of titles and abstracts, followed by a comprehensive assessment of the full-text versions to ensure their alignment with the research objectives. During this stage, the search results were filtered and evaluated based on the following Inclusion Criteria:

1) Peer-reviewed articles published between 2019 and 2024.
2) Literature published in either Indonesian or English.
3) Research specifically addressing IT Risk Management using the NIST Framework, available in a full-paper format.
4) Articles published in accredited international or national journals.

Data Extraction

The data extraction process involves systematically retrieving critical information from the selected scholarly articles to facilitate a rigorous synthesis. For each study included in the final review, specific data points were recorded, including the article title, author credentials, year of publication, methodological approach, and key research findings. By employing this structured extraction method, researchers and readers can attain a comprehensive and granular understanding of the current state of IT risk management in education. This systematic approach ensures that the synthesized results are grounded in empirical evidence, allowing for a detailed comparison of NIST framework applications across different educational contexts.

Data Analysis and Synthesis

Following the data collection phase, the study proceeded to a systematic analysis aimed at identifying emerging patterns and cross-study thematic trends within the evaluated literature. This analytical process serves to consolidate evidence regarding IT risk assessments and their practical execution. The analysis was conducted by aligning the extracted data with the core pillars of the NIST Risk Management Framework. The synthesis specifically focuses on three critical domains:

1) Evaluating how specialized academic environments apply standardized risk controls.
2) Identifying the systemic, technical, and human-centric obstacles encountered during the implementation of the NIST Framework.
3) Exploring how the NIST Framework interacts with other governance models, such as COBIT, to provide a comprehensive strategy for managing IT risks within educational institutions.

This structured approach ensures that the findings are not merely a summary of individual articles but a synthesized perspective on the current landscape of cybersecurity governance in education.

Report Preparation

In the final stage, the data synthesized from previous phases are utilized to substantiate the research findings through a rigorous analysis of the empirical evidence uncovered. By applying the NIST framework as a lens for evaluation, this process yields critical insights into the current state of IT risk management within the educational sector. The culmination of this study is designed to provide actionable intelligence for practitioners, researchers, and key stakeholders. It is anticipated that these findings will serve as a foundational resource for enhancing IT risk management strategies, fostering more resilient security postures in educational environments globally.

RESULTS AND DISCUSSION

Previous Research

During the literature review process, relevant articles and scholarly works were retrieved from various electronic databases, including Semantic Scholar and Google Scholar. The following table summarizes the key studies that inform the theoretical and practical foundations of this research:

Table 2. Literature Source Screening Results

Source Database	Data Found	Article Candidate	Featured Articles
Google Scolar	471	14	8
Semantic scholar	720	9	7

Literature Selection Results

Following the identification and screening of articles across multiple electronic journal databases, twelve studies were selected that strictly met all established inclusion criteria. This rigorous selection process ensured that the final synthesis is based on high-quality, relevant scholarly work. The table below illustrates the distribution of these articles based on the specific search strings and keywords utilized during the retrieval process.

Table 3. Distribution of Research Keywords

No	Keywords	Database	Reference Literature	Frequency
1.	IT Risk Management NIST	Google Scholar, Semantic Scholar	[1], [4], [7], [10],[11], [14], [18], [19], [20], [21]	10
2.	Education Industry	Google Scholar, Semantic Scholar	[8], [9], [10], [18]	4
3.	NIST IT Risk Management in Education	Google Scholar, Semantic Scholar	[3], [4], [6], [9], [10], [12], [18], [19]	8

Effective NIST Implementation for IT Risk Identification and Mitigation in Educational Institutions within the Digital Era

This study evaluates the effectiveness of risk mitigation utilizing the NIST framework. Current literature suggests that the NIST SP 800-30 framework provides a highly structured methodology for identifying IT risks within educational settings. Research indicates that this approach facilitates risk classification based on impact levels across multiple domains, including technical threats (cyberattacks), operational vulnerabilities (human error), and environmental hazards (natural disasters) [9], [10]. Furthermore, the framework supports robust mitigation strategies through the deployment of technical controls, such as firewalls and data encryption protocols [3], [22]. These findings underscore that the NIST framework offers comprehensive and adaptable guidance for managing the dynamic IT risks inherent in educational environments.

Empirical evidence further demonstrates that the NIST framework can be effectively tailored to address specific educational requirements, such as the management of computer laboratories and the safeguarding of sensitive student data [19], [23]. Notably, research indicates that adopting NIST standards enhances institutional compliance with global data protection regulations, including the General Data Protection Regulation (GDPR) and regional Personal Data Protection Acts [23].

Based on these synthesized results, the implementation of the NIST SP 800-30 framework provides significant advantages in both identifying and mitigating IT risks. The framework offers holistic guidance covering the entire risk management lifecycle, from initial identification to periodic evaluation [1], [23]. Findings across various studies confirm that educational institutions adopting this framework achieve superior data protection outcomes and a measurable reduction in security incidents [18], [19]. In conclusion, this study reveals that the NIST 800-30 framework possesses immense potential to bolster IT risk management in education. While implementation challenges remain, multi-stakeholder collaboration is the fundamental key to achieving sustainable and resilient cybersecurity posture.

Implementation Challenges of NIST Frameworks in the Educational Sector

The implementation of the NIST framework within the educational sector is a highly effective measure for minimizing cyberattack risks. However, the adoption of this framework is not without significant challenges. Several studies identify resource constraints as a primary barrier, particularly for educational institutions in developing nations [1], [8]. Furthermore, low levels of IT security literacy among academic and administrative staff serve as an additional impediment to effective implementation [11]. Technical hurdles also emerge, such as fragmented IT infrastructures and a heavy reliance on legacy systems that are often incompatible with modern security standards [3], [9]. Additionally, overlapping or conflicting regulatory requirements frequently increase the complexity of framework adoption [7].

The success of framework implementation is fundamentally dependent on an institution's ability to navigate these challenges. Resource limitations can be mitigated through collaborative initiatives

between educational institutions and government agencies. Enhancing IT security literacy through continuous and routine training programs is also a critical step, as suggested by recent research [14]. Moreover, the development of policies and regulations that are better synchronized with the specific operational needs of educational institutions will significantly reduce the complexity associated with NIST framework implementation.

CONCLUSION

The implementation of the NIST SP 800-30 framework within educational institutions is an effective strategy for identifying and mitigating technological risks in the digital era. This framework provides structured guidance to address a broad spectrum of vulnerabilities, ranging from technical to environmental factors, while significantly enhancing data security and system integrity. Through systematic research and application, educational institutions can better navigate increasingly complex IT challenges. However, the implementation of this framework also encounters several obstacles, including regulatory complexity, substandard IT security literacy, and significant resource constraints. A collaborative approach involving diverse stakeholders within the educational ecosystem, coupled with routine training programs, serves as an effective solution to these issues. Ultimately, the synergy between all involved parties is essential to ensure a successful, resilient, and incident-free implementation.

REFERENCES

[1] K. MacFarland, "Re: Response to National Institute of Standards and Technology (NIST) Request for Information on Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management," 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:249271963

[2] F. Faizal, "PERANCANGAN TATA KELOLA TEKNOLOGI INFORMASI DI POLITEKNIK LAMANDAU MENGGUNAKAN FRAMEWORK COBIT 5," Jurnal Informatika Polinema, vol. 8, no. 1, pp. 1–8, Nov. 2021, doi: 10.33795/jip.v8i1.610.

[3] M. Mukherjee, N. T. Le, Y.-W. Chow, and W. Susilo, "Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes," Information, vol. 15, no. 2, p. 117, Feb. 2024, doi: 10.3390/info15020117.

[4] A. I. A. Ain, A. Ambarwati, and L. Junaedi, "Analisis Manajemen Risiko Teknologi Informasi dan Keamanan Aset Dengan Menggunakan Nist Sp 800-30 Revisi 1," Jurnal Ilmu Komputer dan Bisnis, vol. 13, no. 2a, pp. 155–165, Dec. 2022, doi: 10.47927/jikb.v13i2a.403.

[5] A. A. Arifnur, H. Heryanto, and Y. Megasyah, "Manajemen Risiko Sistem Informasi Pengarsipan menggunakan NIST SP 800-30 pada Kopertis Wilayah IV Bandung," Jurnal Nasional Teknologi dan Sistem Informasi, vol. 9, no. 2, pp. 208–217, Sep. 2023, doi: 10.25077/TEKNOSI.v9i2.2023.208-217.

[6] A. Mutiarachim, A. Putra Ramdani, A. Zubair, and Y. Maritza, "Manajemen Risiko Digital untuk Keamanan Siber yang Lebih Kuat di Era Industri 4.0-Systematic Literature Review," 2025. [Online]. Available: https://jurnal2.untagsmg.ac.id/index.php/DBIJ

[7] B. Tjahjono, M. Ardiansyah, G. Firmansyah, and H. Akbar, "Risk Management Of Information System In Diskominfo Statistic And Encoding Using NIST SP 800-30," JITK (Jurnal Ilmu Pengetahuan dan Teknologi Komputer), vol. 9, no. 1, pp. 134–142, 2023.

[8] A. M. Amine, E. M. Chakir, T. Issam, and Y. I. Khamlichi, "A Review of Cybersecurity Management Standards Applied in Higher Education Institutions," International Journal of Safety and Security Engineering, vol. 13, no. 6, pp. 1109–1116, Dec. 2023, doi: 10.18280/ijsse.130614.

[9] C. E. Bondoc and T. G. Malawit, "Cybersecurity for higher education institutions: adopting regulatory framework," Global Journal of Engineering and Technology Advances, 2020, [Online]. Available: https://api.semanticscholar.org/CorpusID:216276753

[10] T. Y. Khaw and A. P. Teoh, "Risk management in higher education research: a systematic literature review," Quality Assurance in Education, 2022, [Online]. Available: https://api.semanticscholar.org/CorpusID:251689982

[11] A. E. S. Setyadji et al., "CAUSES OF INEFFECTIVE IMPLEMENTATION OF IT GOVERNANCE IN RISK MANAGEMENT: A SYSTEMATIC LITERATURE REVIEW," JIKO (Jurnal Informatika dan Komputer), vol. 6, no. 2, Aug. 2023, doi: 10.33387/jiko.v6i2.6182.

[12] M. H. Fadhillah, "Risk Mitigation of Academic Information System in XYZ University," Jurnal Sistem Informasi, Manajemen, dan Akuntansi (SIMAK) , 2024, doi: 10.35129/simak.v22i01.480.

[13] U. Nugraha and R. Istambul, "Implementation of ISO 31000 for Information Technology Risk Management in the Government Environment," 2019. [Online]. Available: www.ijicc.net
[14] J. V. Barraza de la Paz, L. A. Rodríguez-Picón, V. Morales-Rocha, and S. V. Torres-Argüelles, "A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0," Systems, vol. 11, no. 5, p. 218, Apr. 2023, doi: 10.3390/systems11050218.
[15] "Systematic Literature Review," in Encyclopedia of Public Health, Dordrecht: Springer Netherlands, 2008, pp. 1376–1376. doi: 10.1007/978-1-4020-5614-7_3433.
[16] F. Z. Nisa', G. D. Febrianti, and N. N. Ajrina, "Systematic Literature Review: Analisis Implementasi Manajemen Risiko TI Menggunakan Framework COBIT di Sektor Industri Jasa," Bulletin of Computer Science Research, vol. 4, no. 1, pp. 66–74, Dec. 2023, doi: 10.47065/bulletincsr.v4i1.313.
[17] B. Belmoukari, J.-F. Audy, and P. Forget, "Smart port: a systematic literature review," European Transport Research Review, vol. 15, no. 1, p. 4, Mar. 2023, doi: 10.1186/s12544-023-00581-6.
[18] R. Farismana and D. Pramadhana, "Risk Management in Final Semester Exam Information System Using NIST 800-30 Method (Case Study of SMKN 2 Baleendah)," Jurnal Ilmu Komputer An Nuur, vol. 2, 2022.
[19] N. Addinillah and F. Sulianta, "ANALISIS MANAJEMEN RISIKO MENGGUNAKAN METODE NIST 800-30 PADA LAB KOMPUTER SEKOLAH (Studi Kasus: SMP Negeri 1 Ciniru)," Jan. 2024.
[20] M. A. Septiawan, A. Dermawan, A. Nur, A. Phasya, A. A. Adipermana, and U. Nugraha, "Risk Management of Outdoor Equipment Rental Information System Using NIST SP 800-30 Framework at PT. XYZ," Sistem Informasi dan Teknologi Informasi, vol. 2, no. 1, 2024, doi: 10.33197/justinfo.v2i1.1743.
[21] N. W. Marbun, F. A. Iz, M. Ramadhan, L. J. H. Kogoya, L. F. Nugraha, and U. Nugraha, "Payment and Transaction Risk Management at Coffeeshop X Using NIST 800-30 Framework," JUSTINFO | Jurnal Sistem Informasi dan Teknologi Informasi, vol. 1, no. 2, pp. 135–146, Jun. 2024, doi: 10.33197/justinfo.vol1.iss2.2023.1745.
[22] A. A. Arifnur, H. Heryanto, and Y. Megasyah, "Manajemen Risiko Sistem Informasi Pengarsipan menggunakan NIST SP 800-30 pada Kopertis Wilayah IV Bandung," Jurnal Nasional Teknologi dan Sistem Informasi, vol. 9, no. 2, pp. 208–217, Sep. 2023, doi: 10.25077/teknosi.v9i2.2023.208-217.
[23] I. E. Nurdin and B. Soewito, "DEVELOPMENT OF AN INTEGRATED IT RISK MANAGEMENT FRAMEWORK FOR ELECTRONIC-BASED GOVERNMENT SYSTEMS: A CASE STUDY OF THE XYZ MINISTRY," 2024.