DOI: https://doi.org/10.33197/justinfo.v3i1.2544 ISSN: 3031-3449

Cyber Risk Mitigation Strategy for Cybernetic PC Gaming Based on the NIST 800-30 Framework

[1] Rizky Alberto Evangelista Pardede, [2] Ucu Nugraha
[1] Information Systems, Faculty of Engineering, Widyatama University, Bandung, Indonesia, rizky.pardede@widyaatama.ac.id
[2] Information Systems, Faculty of Engineering, Widyatama University, Bandung, Indonesia, ucu.nugraha@widyatama.ac.id

ABSTRACT

The operational dependency of internet cafes (gaming centers) on Information Technology (IT) infrastructure creates significant risk exposure to business continuity and data security. Cybernetic PC Gaming, a gaming service provider in Bandung, faces challenges in the form of cyber threats and physical disruptions that have the potential to damage its reputation and financial standing. This study aims to identify, analyze, and evaluate the level of information security risk by applying the National Institute of Standards and Technology (NIST) Special Publication 800-30 framework. The research method employed is descriptive qualitative, encompassing the nine stages of risk management, from system characterization to mitigation results documentation. The study successfully identified five primary risk profiles. Based on risk matrix calculations, two threats were classified at a "High" level: power outages lacking adequate backup power support and the risk of malware infection from customers downloading harmful files. Meanwhile, internet connection disruptions, natural disasters, and hardware dust accumulation were rated at a "Moderate" level. As a solution, this research formulates strategic control recommendations, including the procurement of a backup generator, internet service provider (ISP) redundancy, and the implementation of web filtering and enterprise-grade antivirus software. In conclusion, the systematic application of the NIST 800-30 standard can transform risk management at Cybernetic PC Gaming from a reactive to a proactive approach, thereby ensuring operational resilience and sustainable protection of digital assets.

Keywords: Risk Management, NIST 800-30, Internet Café, Information Security, Mitigation.

Corresponding Author:

Rizky Alberto Evangelista Pardede
Information Systems, Faculty of Engineering, Widyatama University
Bandung, Indonesia
rizky.pardede@widyaatama.ac.id

INTRODUCTION

In the current era of digital transformation, internet cafés (warnet) have evolved into centers for entertainment and high-performance computing through the gaming center concept [1]. Cybernetic PC Gaming is one such business entity that relies on Information Technology (IT) infrastructure as the backbone of its services. This massive dependence on information systems creates significant risk exposure, encompassing cyber threats, systemic failures, and physical vulnerabilities [2]. Disruptions to IT infrastructure not only result in short-term financial losses but can also damage business reputation and erode long-term customer trust.

Risk management in small to medium-sized business sectors has been extensively researched using various frameworks. Previous studies have frequently adopted standards such as ISO 31000 or COBIT 5 for managing IT governance in a general sense [3]. However, within the more technical and in-depth context of information security, the National Institute of Standards and Technology (NIST) Special Publication 800-30 framework is recognized as the gold standard [4]. It provides a highly structured methodology, ranging from system characterization to control identification. This standard

has proven effective in mitigating risks for large organizations and government agencies in various developed countries.

Although research on NIST 800-30 is abundant, most case studies remain focused on banking, healthcare, or governmental institutions. A literature gap exists regarding the application of cyber risk management to digital Micro, Small, and Medium Enterprises (MSMEs) such as gaming centers [5]. The risk profile of a gaming center is highly unique, involving high data traffic loads, vulnerabilities from third-party software (games), and intensive physical customer interaction factors seldom encountered in formal corporate sectors [6].

The novelty of this research lies in the adaptation and practical implementation of the NIST 800-30 framework to the gaming center business model, which operates locally yet possesses technical complexity equivalent to mid-scale network infrastructure. This study not only maps risks theoretically but also provides tailored, cost-effective, and applicable security controls for the MSME scale a sector often perceived as too complex for adopting the full NIST standard.

Based on this background, this research aims to identify and analyze the specific risk profile at Cybernetic PC Gaming. More specifically, the study intends to evaluate the effectiveness of existing controls and formulate NIST 800-30-based risk mitigation strategy recommendations. The outcomes of this research are expected to serve as a practical guide for gaming center management to enhance system resilience and ensure business continuity amidst evolving cyber threats.

LITERATURE REVIEW

Risk management is a systematic approach encompassing the identification, evaluation, and control of threats to ensure organizational operational continuity. Yuwono & Ellitan (2025) asserts that the primary objective of risk management is to manage uncertainty so that its negative impacts can be minimized [7]. In the digital era, Information Systems Risk Management (ISRM) has become a crucial element due to organizations' increasing dependence on technological infrastructure [8]. ISRM does not solely focus on technical aspects but also integrates human and procedural elements in protecting valuable information assets.

The National Institute of Standards and Technology (NIST) Special Publication 800-30 is a globally recognized, comprehensive guideline for IT risk management. This framework offers a structured methodology through nine primary stages: (1) system characterization, (2) threat identification, (3) vulnerability identification, (4) control analysis, (5) likelihood determination, (6) impact analysis, (7) risk determination, (8) control recommendations, and (9) results documentation [9]. The strength of NIST 800-30 lies in its ability to convert qualitative threats into measurable risk assessments, thereby facilitating strategic decision-making [10], [11].

The operational context of internet cafés or gaming centers possesses specific risk characteristics. Aslan et al. (2023) identify that major threats in this sector include cyber-attacks such as malware and phishing, hardware failures, and physical threats such as theft of hardware components [12]. Furthermore, external factors such as instability of electrical power supply and limitations in human resource competency for security management also constitute significant risk variables [13]. Research on risk management using NIST 800-30 has advanced significantly over the last decade. Table 1 summarizes the evolution of related research that forms the foundation for this study's position:

Table 1. Comparison of Related Research (State of the Art)

Researcher (Year)	Research Object	Framework	Key Findings / Results
Hermawan et al. (2025) [8]	Government Institutions	NIST 800-30	Focus on Information assets in the information system at the data center.
Elanda & Buana (2021) [9]	Educations Institutions	NIST 800-30	Found that risk management increased operational efficiency by 30%.
Arifnur et al. (2023) [13]	Critical Infrastructure	NIST 800-30	Emphasized physical risks and natural disasters on data centers.
This Research (2025)	Cybernetic PC Gaming	NIST 800-30	Adaptation of specific security controls for gaming centers with high data traffic.

The current state of the art demonstrates a transition in the use of NIST 800-30 from large-scale organizations to medium and micro business units. Nonetheless, a gap remains in the literature specifically addressing the application of this standard to the gaming center ecosystem, which features high-bandwidth network complexity and security risks from public users. This study addresses that gap by adapting the nine steps of NIST 800-30 to the operational characteristics of Cybernetic PC Gaming, aiming to produce more applicable and cost-effective control recommendations.

METHODOLOGY

This study employs a descriptive qualitative method, adopting the National Institute of Standards and Technology (NIST) Special Publication 800-30 framework as the primary instrument for risk assessment [5]. The research flow commences with the system characterization stage, involving a comprehensive identification of information technology assets at Cybernetic PC Gaming, including hardware, software, and customer data flows. Once the system boundaries are established, a threat identification is conducted to map potential disruptions from human, natural, or environmental factors. This is then synchronized with the vulnerability identification stage to uncover weaknesses in the existing network infrastructure and operational procedures. Subsequently, a control analysis is performed to evaluate the effectiveness of currently implemented protective measures. Based on these findings, a likelihood determination and an impact analysis are conducted using a qualitative scale to measure the potential frequency of threat occurrence and the magnitude of losses incurred across the aspects of confidentiality, integrity, and availability. The synthesis of these two parameters is utilized to perform a risk determination. Mathematically, the risk level is calculated by multiplying the likelihood weight by the impact weight, according to the following formula:

$$R = L \; x \; I \tag{1}$$

Where R (Risk) represents the resulting risk level, L (Likelihood) is the probability value of a threat occurring, and I (Impact) is the magnitude of the impact on business operations. The results of this calculation are then mapped onto a risk matrix to determine the priority scale for mitigation. This is followed by the formulation of mitigating control recommendations. The entire research process concludes with results documentation to serve as the foundation for strategic decision-making by the management of Cybernetic PC Gaming.

RESULTS

Risk management was implemented at Cybernetic PC Gaming systematically through the nine stages of the NIST 800-30 framework. The following presents the analysis results.

System Characterization

The initial stage involved identifying critical assets supporting business operations. Cybernetic PC Gaming manages integrated physical and software assets to deliver gaming and administrative services.

Physical Assets

The physical infrastructure consists of 14 Premium PC units (Intel i3/RX 580) and 10 VIP PC units (Intel i5/GTX 1660 Super). Supporting equipment includes Asus ROG Swift monitors, Rexus-brand peripherals, and network infrastructure comprising 3 modem/router units. For security and management, assets include 8 CCTV units, a cash register, and 2 Uninterruptible Power Supply (UPS) units dedicated to the server and administration PC to ensure transaction continuity during power disruptions.

Software Assets

The operational system uses CafeIndo software for billing and member data management. Additionally, VMS Lite is utilized for real-time CCTV monitoring integration, while Microsoft Excel and the QRIS (Quick Response Code Indonesian Standard) digital payment system are employed for administrative efficiency and transactions.

Threat Identification

Threats were categorized into three primary domains, as detailed in Table 2.

Table 2. Threat Identification

Threat Category	Example Threats	Potential Consequence
Natural Disaster	Flood, Earthquake, Fire	Permanent hardware damage and data loss.
Physical Security	Asset theft, Customer negligence	Loss of physical assets and high replacement costs.
Cybersecurity	Malware, Phishing, DDoS attacks	Customer data breach and system service disruption.

Vulnerability Identification and Control Analysis

Observations revealed several critical vulnerabilities, including a high dependency on a single Internet Service Provider (ISP) and dust accumulation on devices, which can degrade hardware performance. The control analysis indicated that existing mitigations are partial; for instance, UPS coverage is limited to the administration PC, and there is no backup generator for the entire system.

Table 3. Vulnerability Identification

No.	Vulnerability	Potential Impact
1	Internet Connection Disruption	Service interruption and disruption of customer activities.
2	Natural Disasters (e.g., flood)	Hardware damage and data loss.
3	Hardware Failure Due to Dust Accumulation	Reduced device performance and increased maintenance costs.
4	Downloading of Harmful Files by Customers	Vulnerability to malware that can steal or corrupt critical data.
5	Power Outage	Data loss and operational disruption.

Table 4. Control Analysis

No.	Risk	Existing Control Measures
1	Internet Connection Disruption	Provision of backup internet connection and periodic network monitoring.
2	Natural Disasters (e.g., flood)	Implementation of physical safeguards, such as locating equipment in elevated areas.
3	Hardware Failure Due to Dust Accumulation	Routine device cleaning and the use of dust filters.
4	Downloading of Harmful Files by Customers	Installation of antivirus software and restriction of access to suspicious websites.
5	Power Outage	Use of Uninterruptible Power Supply (UPS) units and backup generators to ensure operational continuity.

Likelihood Determination and Impact Analysis

The likelihood and impact levels were determined to quantify the identified risks, as summarized in Table 5.

Table 5. Risk Likelihood and Impact Assessment

No.	Potential Risk	Likelihood	Impact	Risk Level
1	Internet Connection Disruption	Moderate	Moderate	Moderate
2	Natural Disaster (Flood)	Low	High	Moderate
3	Hardware Dust Accumulation	Moderate	High	Moderate
4	Downloading Harmful Files	High	High	High
5	Power Outage	High	High	High

Risk Determination and Control Recommendations

The analysis identified two risks in the High category: power outages and customer activities involving the download of harmful files. Recommended mitigation strategies are categorized as follows:

1) Technical: Installation of enterprise-grade antivirus software and implementation of web filtering to prevent malware intrusion.
2) Infrastructural: Procurement of a backup generator or incremental expansion of UPS capacity to ensure service availability.
3) Procedural: Scheduling regular physical maintenance (e.g., deep cleaning) to prevent dust-related damage and optimizing backup ISP connectivity.

Following the risk level determination, a comprehensive mitigation strategy was developed. According to the NIST 800-30 standard, each identified risk was prioritized based on its urgency. The proposed mitigation plan is detailed in Table 6.

Table 6. Cybernetic PC Gaming Risk Mitigation Plan

Risk	Risk Level	Recommended Control	Priority	Resources & Responsible
Internet Disconnection/Lag	High	• Add network devices from a different provider (redundancy). • Repair/upgrade old routers. • Implement regular periodic restarts.	High	4 Days; Owner & Network Technician
Downloading Harmful Files (Malware)	High	• Install updated antivirus software. • Block malicious sites via firewall or browser settings.	High	6 Hours; Admin & Owner
Power Outage	High	• Procure a generator unit. • Install UPS on each PC for power stability.	High	1 Day; Owner & Electrical Technician
Flood (Clogged Drainage)	Moderate	• Perform regular drainage channel cleaning. • Install automatic water pumps in prone areas.	Moderate	6 Hours; Owner & Plumbing Technician
Hardware Dust Accumulation	Moderate	• Conduct routine device and room cleaning. • Install dust filters on PC and server casings.	Moderate	4 Hours; Owner & Cleaning Service

Mitigation efforts are primarily focused on network stability, data security from malware, and power continuity. Addressing internet connectivity and power outages requires coordination with specialized technicians due to the need for new infrastructure installation (e.g., generators, additional routers). To maintain control effectiveness, Cybernetic PC Gaming must implement a routine maintenance schedule. This includes weekly router performance monitoring, regular antivirus database updates, and bi-annual maintenance of UPS and generator units to ensure optimal performance. Moderate risks, such as dust accumulation and flood threats, are addressed through procedural preventive actions, including establishing a weekly cleaning schedule and evaluating the drainage system every three months.

Results Documentation

This risk assessment report provides a strategic guide for the management of Cybernetic PC Gaming. The primary mitigation focus is directed toward the aspects of Availability (power and internet) and Integrity (data protection from malware). Implementing these recommendations is expected to significantly enhance the operational resilience of the business.

DISCUSSION

The risk analysis at Cybernetic PC Gaming indicates that cybersecurity threats and infrastructure instability represent the highest-level risks requiring immediate action. This finding aligns with the research by Hermawan et al. (2025), which states that an organization's reliance on technology is directly proportional to the scale of functional impact in the event of a system failure. At Cybernetic PC Gaming, the "High" risk rating for power outages and internet disruptions confirms that availability is the foremost priority for a digital service business.

Regarding cybersecurity, the risk of customers downloading harmful files was identified as a critical threat. This confirms the theory proposed by Aslan et al. (2023), which emphasizes that public internet cafe environments are highly vulnerable to malware due to unrestricted public access. However, this study offers more specific solutions compared to prior research by recommending the implementation of combined firewall and web filtering measures, alongside regular antivirus database updates.

The application of the NIST 800-30 framework in this study proved effective in transforming qualitative threats into measurable action plans. This finding is consistent with the results of Elanda & Buana (2021), who demonstrated that implementing NIST standards provides a clearer mitigation structure for MSMEs compared to ad-hoc methods. A significant distinction in this study lies in the adaptation of physical controls, such as the use of dust filters and ambient temperature management (air conditioning), measures that Arifnur et al. (2023) argue are often overlooked yet have a substantial impact on the lifespan of digital assets in high-user-traffic environments.

Overall, the proposed mitigation strategies, such as procuring backup generator units and adding internet provider redundancy, are designed not only to reduce risk but also to enhance the business's competitive value in the eyes of customers. By implementing the recommendations derived from the nine-step NIST 800-30 process, Cybernetic PC Gaming can transition from a reactive to a proactive risk management posture, thereby ensuring long-term business sustainability amid an evolving landscape of threats.

CONCLUSION

This study successfully implemented the nine-step risk management process based on the NIST 800-30 framework at Cybernetic PC Gaming. Based on the conducted analysis, the following conclusions can be drawn:

1) The asset identification revealed that business continuity is heavily reliant on IT infrastructure (Premium and VIP PCs) and management software such as CafeIndo.
2) Five primary risks were identified, with two categorized as High: the threat of power outages and the cybersecurity risk stemming from customers downloading harmful files.
3) The application of the risk formula, R=L×I, provided an objective basis for management to prioritize mitigation efforts focusing on availability (service continuity) and integrity (system and data integrity).
4) The proposed control recommendations including the procurement of a backup generator, ISP redundancy, and the enhancement of antivirus and web filtering prove to be both practical and strategic solutions for improving the operational resilience of the business.

Based on the research findings, several recommendations are proposed for the management of Cybernetic PC Gaming and for future researchers:

1) It is advised to promptly begin the phased procurement of additional UPS units and a backup generator. Furthermore, implementing a routine schedule for physical device maintenance (e.g., deep cleaning) every three months is crucial to maintain optimal hardware performance.
2) Periodic training on basic cybersecurity procedures is recommended for administrators. This will enhance their ability to effectively monitor customer activities on the network and respond to potential threats.
3) It is suggested to conduct a Cost-Benefit Analysis (CBA) on the provided control recommendations to measure the financial efficiency of each proposed security investment. Additionally, future research could explore integrating this risk management approach with other international security standards, such as ISO/IEC 27001.

REFERENCES

[1] T. O. Wibowo, W. Udasmoro, and R. Noviani, "Understanding new consumption sites of internet cafe in Yogyakarta, Indonesia," *J. Ilmu Sos. dan Ilmu Polit.*, vol. 23, no. 3, pp. 237–249, 2020, doi: 10.22146/jsp.51707.

[2] Istikhomah and Y. N. Kunang, "Analisis Manajemen Risiko Sistem Informasi Akademik Dengan Menggunakan Metode NIST SP 800-30 Revisi 1 (Studi Kasus: Universitas Bina Darma)," vol. 1, pp. 1–10, 2023, [Online]. Available: http://repository.binadarma.ac.id/id/eprint/7632%0Ahttp://repository.binadarma.ac.id/7632/5/Artikel jurnal %26 LOA.pdf

[3] U. Nugraha and R. Istambul, "Implementation of ISO 31000 for information technology risk management in the government environment," *Int. J. Innov. Creat. Chang.*, vol. 6, no. 5, pp. 219–231, 2019.

[4] C. Asari and Yulhendri, "Manajemen Risiko Sistem Informasi Mengacu pada NIST SP 800-30 dan NIST SP 800-53 rev.5," *J. Teknol. Dan Sist. Inf. Bisnis*, vol. 5, no. 4, pp. 420–430, 2023, doi: 10.47233/jteksis.v5i4.898.

[5] R. Gimnastiar, R. Nursyanti, and S. Sardjono, "Audit Keamanan Dan Manajemen Risiko Dengan Menggunakan Framework NIST (Studi Kasus: E-Learning UNIBI)," in *Seminar Nasional Corisindo*, Bandung: Universitas Teknologi Bandung, 2024, pp. 148–153. [Online]. Available:

https://corisindo.utb-univ.ac.id/index.php/penelitian/article/view/61%0Ahttps://corisindo.utb-univ.ac.id/index.php/penelitian/article/download/61/25

[6] V. ÇAKMAK and E. AKTAN, "Internet Cafes, Young People and Game Interaction: a Study in the Context of Subculture," *MANAS Sos. Araştırmalar Derg.*, vol. 7, no. 3, pp. 0–0, 2018.

[7] M. A. Yuwono and L. Ellitan, "Implementation of Enterprise Risk Management As a Strategy for Increasing Competitive Advantage: Study At Companies in Central Kalimantan," *J. Bus. Manag. Account.*, vol. 15, no. 1, pp. 55–78, 2025, [Online]. Available: https://doi.org/10.32890/jbma2025.15.1.4

[8] I. Hermawan, B. T. Hanggara, and A. R. Perdanakusuma, "Manajemen Risiko Sistem Informasi Menggunakan Metode NIST SP 800 – 30 Studi Kasus Pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 9, no. 6, pp. 1–10, 2025, [Online]. Available: http://j-ptiik.ub.ac.id

[9] A. Elanda and R. L. Buana, "Analisis Manajemen Risiko Infrastruktur Dengan Metode NIST (National Institute of Standards and Technology) SP 800-30 (Studi Kasus : STMIK Rosma)," *Elkom J. Elektron. dan Komput.*, vol. 14, no. 1, pp. 141–151, 2021, doi: 10.51903/elkom.v14i1.387.

[10] H. Ben Ameur, Z. Ftiti, and W. Louhichi, "Do ESG investments improve portfolio diversification and risk management during times of uncertainty," *J. Int. Financ. Mark. Institutions Money*, vol. 103, p. 102199, 2025, doi: https://doi.org/10.1016/j.intfin.2025.102199.

[11] M. L. Gathigia and M. A.-M. Wairimu, "RISK MANAGEMENT PRACTICES AND PERFORMANCE OF INFRASTRUCTURAL PROJECTS IN NAKURU COUNTY, KENYA," *Int J. Soc. Sci. Manag. Entrep.*, vol. 7, no. 1, pp. 457–469, 2023, [Online]. Available: www.sagepublishers.com

[12] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electron.*, vol. 12, no. 6, 2023, doi: 10.3390/electronics12061333.

[13] A. A. Arifnur, H. Heryanto, and Y. Megasyah, "Manajemen Risiko Sistem Informasi Pengarsipan menggunakan NIST SP 800-30 pada Kopertis Wilayah IV Bandung," *J. Nas. Teknol. dan Sist. Inf.*, vol. 9, no. 2, pp. 208–217, 2023, doi: 10.25077/teknosi.v9i2.2023.208-217.