International Journal of Informatics and Computation (IJICOM)
Vol. 8, No. 1, 2026
ISSN: 2685-8711, E-ISSN: 2714-5263 DOI: 10.35842/ijicom

Increasing Technical Justification for University's Data Center Development

I Putu Deny Arthawan Sugih Prabowo[1], Riska Kurniyanto Abdullah[2], I Nengah Suweden[3], Yesi Destri Seppang[4], Dwi Arief Prambudi[5], M. Chandra Cahyo Utomo[6], Arum Kurnia Sulistyawati[7], Jeffry Andhika Putra[8], Adiek Astika Clara Sudarni[9]

Abstract
Resilient information technology (IT) infrastructure is required for the digitalization of higher education to support essential academic and administrative IT services. XYZ University faced significant challenges due to vulnerabilities in its existing data center, which lacked standardized technical qualifications and was susceptible to single points of failure. This study formulated a comprehensive technical justification for developing a Tier-3 data center by synthesizing the technical references/standards and adapting risk management best practices from the Indonesian banking sector. The findings indicated that in achieving concurrent maintainability and 99.982% availability, critical infrastructure requirements must be met in the architectural, electrical, mechanical (HVAC), and telecommunications domains. N+1 redundancy, 500 kVA backup power, and grounding of less than 1 ohm are all important parts that keep XYZ University's important IT services, such as SIAKAD and LMS, safe. These justifications served as the foundational reference for the institutional Disaster Recovery Plan (DRP). The study concluded a Rector's Decree that incorporates technical references/standards into strategic strategy offers a strong governance framework for the academic community as a whole to ensure long-term digital resilience and the continuity of IT services.

Keywords:
Data Center, DRP, IT services, XYZ University, Technical Justification

1. Introduction

A university in a city/regency of East Kalimantan Province called XYZ University, where it is also located near to New Indonesian National Capital of Nusantara. For XYZ University, dependence on information technology (IT) services is no longer a secondary issue but a fundamental prerequisite for the successful implementation of the higher education's "Tridharma" activities, such as the activities of implementing education, scientific studies/research, and community service. To support the continuity of IT services that support operations or business processes at XYZ University, including academic business processes which are the "core business processes" of XYZ University, the supports for the availability of XYZ University's IT resources is very much needed, especially the capable XYZ University's IT infrastructures. Thus, the availability of a data center that meets the minimum technical requirements of Tier-3 is also very necessary to support XYZ University's IT services continuity [1], [2], [3], [4].

Corresponding Authors:
1 I Putu Deny Arthawan Sugih Prabowo, Department of Information Systems, Institut Teknologi Kalimantan, putudeny.asp@lecturer.itk.ac.id
2 Riska Kurniyanto Abdullah, Department of Informatics, Institut Teknologi Kalimantan, riska.abdullah@lecturer.itk.ac.id
3 I Nengah Suweden, PT. Sari Mertha Luwih (a MEP/MEPIT Consultant Company in Indonesia).
4 Yesi Destri Seppang, Department of Information Systems, Institut Teknologi Kalimantan, 10211087@student.itk.ac.id
5 Dwi Arief Prambudi, Department of Information Systems, Institut Teknologi Kalimantan, dwiariefprambudi@lecturer.itk.ac.id
6 M. Chandra Cahyo Utomo, Department of Informatics, Institut Teknologi Kalimantan, ccahyo@lecturer.itk.ac.id
7 Arum Kurnia Sulistyawati, Department of Information Systems, Universitas Respati Yogyakarta, arumkurnia@respati.ac.id
8 Jeffry Andhika Putra, Department of Digital Business, Universitas Janabadra Yogyakarta, jeffry@janabadra.ac.id
9 Adiek Astika Clara Sudarni, Department of Safety Engineering, Institut Teknologi Kalimantan, adiek.astika@lecturer.itk.ac.id

The state of IT infrastructure at XYZ University previously revealed a significant gap between the escalating demand for digital services and the physical capabilities of existing facilities. The server room managed by XYZ University's IT Academic Support Unit, did not have the essential technical qualifications of Tier-3, which refers to ANSI/TIA-942 [2] and SNI 8799 [3], [4], as well as other related technical references/standards. Thus, this existing condition had IT risks, including the operational and security of XYZ University's IT services (i.e., IT services related to academic business processes as XYZ University's core business processes) [1], [5], [6], [7], [8], [9], [10].

The urgent need to prepare technical justifications for the development of IT infrastructures, including the XYZ University's data center, was based on empirical evidence of IT service disruptions that had occurred at XYZ University. One such incident involved the accidental severing of fiber optic (FO) cables between the Rectorate Building and the Integrated Laboratory Building during a campus construction project. This event, which stemmed from a violation of standard project management work procedures [11], resulted in a total loss of internet connectivity in key areas, severely hampering the productivity of the entire academic community [1], [12]. Additionally, frequent instances of main power failures on campus further destabilized the continuity of strategic services such as XYZ University’s Learning Management System (LMS) and Academic Information Systems (SIAKAD).

In response to these infrastructure conditions, the development of a Tier-3 data center was proposed as a strategic need for XYZ University. A Tier-3 facility is defined by its "concurrently maintainable" infrastructure, which allows for any component of the power or cooling system to be taken offline for maintenance, repair, or replacement without impacting the operational status of the servers [1], [2], [3], [4], [12]. By establishing technical justifications aligned with international benchmarks (referring to relevant technical references/standards), XYZ University aims to eliminate single-point failures and provide an uptime guarantee of 99.982%, which means no more than 1.6 hours of cumulative downtime per year [1].

Furthermore, the methodology for this technical justification drew from the technical references/standards [1], [2], [3], [4], [8], [9], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], including the regulatory compliance in the banking sector by Indonesian Financial Services Authority (OJK) that mandates a level of risk oversight and disaster recovery capability that is far more stringent than typical academic environments [25], [26], [27]. By adapting "best practices" from a case study of a Regional Development Bank (BPD) [1], XYZ University adopted a posture of extreme reliability. This strategic alignment ensured that the university's data center development was not merely an engineering project but a component of a larger, institutionalized Disaster Recovery Plan (DRP) [1], [12]. This DRP was subsequently formalized via a Rector of XYZ University’s Decree, signaling a top-level commitment to the continuous availability of IT services for the entire academic community.

2. Related Works

As explained in Table 1, the design and implementation of modern data centers are governed by the technical references/standards [1], [2], [3], [4], [8], [9], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], addressing physical security, electrical redundancy, and HVAC (heating, ventilation, and air conditioning) management. At the “forefront” is both ANSI/TIA-942 and SNI 8799 [2], [3], [4]. This study noted that while Tier-1 and Tier-2 facilities might suffice for small entities [1], [2], [3], [4], they were inherently

unsuitable for XYZ University because they required full system shutdowns for maintenance. A Tier-3 facility introduced "Concurrent Maintainability," requiring dual-powered equipment and multiple independent distribution paths [1], [2], [3], [4], [15], [28].

SNI 8799:2023 [3], [4] serves as the benchmark for data center management. A critical technical requirement identified in this study was the mandate for grounding resistance to be less than 1 ohm [3]. This necessitated a dedicated building for the data center at XYZ University, as general-purpose buildings typically only tolerate 5 ohms [3], [24]. Furthermore, thermal management followed ASHRAE 2021 guidelines to prevent hardware degradation [23].

The technical justification also integrated OJK's regulations about risk management in banking sector (including IT risk management) [25], [26], [27], which requires institutions to maintain both a primary data center and a Disaster Recovery Center (DRC) supported by a tested DRP. This mapping allowed XYZ University to treat academic data with the same criticality as financial assets, elevating the standard of institutional information governance [1].

Table 1. References study matrix for compiling technical justification for the development of XYZ University's Data Center

Main Parts of the Technical Justifications	Main References	Secondary References
IT Infrastructures Design	[2], [3], [4], [13], [14], [15], [16], [19], [20], [21], [23], [29], [30]	[1], [28], [31], [32], [33]
IT Security and Risks Management	[8], [9], [16], [17], [19], [20], [21], [22]	[5], [6], [25], [26], [27], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45]
DRP	[12], [17], [18]	[1], [46]

3. Proposed Method

The methodology for developing this technical justification followed a systematic workflow, as shown on **Fig. 1.**, initiated with a comprehensive review of pertinent literatures/standards to establish a robust foundation for XYZ University's Data Center. Beyond utilizing SNI 8799 and ANSI/TIA-942 as primary benchmarks, this study synthesized a diverse range of international standards/references to ensure the technical rigor of the framework. The analysis focused on meeting the stringent requirements for a Tier-3 higher education data center, specifically regarding redundancy and concurrent maintainability, which serve as pivotal elements within XYZ University's DRP Guidelines.

The synthesis of these national and international standards/references ensured that the resulting technical justifications possesses high validity for implementation as a formalized standard for XYZ University's IT infrastructure. Following the initial formulation, the draft underwent a validation phase through the intensive consultation with the Review Committee for XYZ University's IT Technical Justification and DRP Guidelines. During this stage, the draft was iteratively evaluated through a rigorous revision mechanism to ensure the precision of every technical parameter before proceeding to the institutional review level.

After consensus was reached on the initial draft of the technical justification within the technical justification committee/team, the draft was then formally discussed with university leadership to align the technical specifications with the organization's strategic policies

(XYZ University's Strategic Planning). Then, the final phase of the study culminated in the institutional ratification of the document via an XYZ University Rector's Decree. By virtue of this decree, the technical justifications were established as an integral component of XYZ University's DRP Guidelines, thereby mandating its application as a primary reference for DRP executions across the university environment.

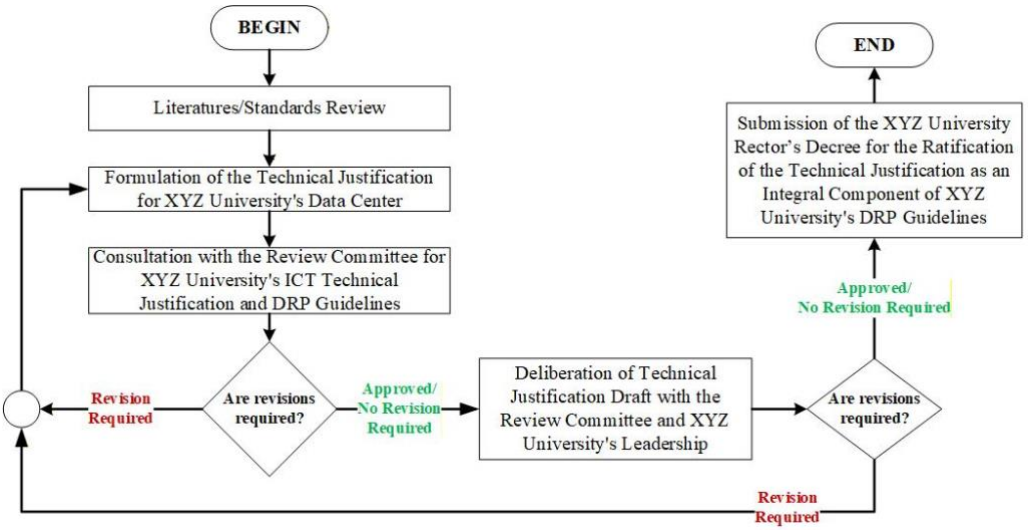

Fig. 1. Study Workflow for the Technical Justification Formulation

4. Result and Analysis

4.1. Domain-Specific Technical Justifications and Implementation

The core findings demonstrate the realization of a Tier-3 XYZ University's data center across four primary domains, ensuring "concurrent maintainability" where any component is serviced without disrupting XYZ University's academic operations or business processes.

1. **Architectural and Site Specifications.**
   The structural isolations and risk mitigations of XYZ University's data center are given top priority in the architectural justifications. According to the technical justifications, the facility was designed as a dedicated building to support specialized grounding loads, which multi-function buildings cannot accommodate, in accordance with SNI 8799 and ASNI/TIA-942. The data center was classified as a "super critical risk" zone in accordance with ISO 31000:2018 and ISO 27001:2022. The installation of 4K CCTV systems with a 30-day retention period was therefore justified as a necessary physical security measure to keep an eye on and document all activity within the server and UPS rooms, safeguarding vital resources against sabotage or illegal access.

2. **Electrical Distribution and Redundancy**
   The electrical system of XYZ University's data center focuses on "eliminating power losses" through an N+1 configuration. This study justified the use of a 500 kVA generator unit that could run continuously for 72 hours as well as two separate power lines from the utility provider (PLN). By not depending entirely on the main power line,

this backup power guarantees that facilities meet Tier-3 availability. In addition, the use of Uninterruptible Power Supply Systems (UPS) in data centers is part of a "delay mechanism" when electrical downtime occurs which has the potential to damage electronic/IT devices (i.e., servers, routers, firewalls, and switches) in the data center. The data center's grounding system was also designed to stay ≤ 1 ohm to protect against surges.

3. **Mechanical and HVAC Systems**
   To control the thermal stress of high-density hardware, mechanical analysis in this technical justification concentrated on precise cooling system in data center. This technical justification set a required temperature range of 18°C to 27°C and a relative humidity of 40% to 60% in accordance with ASHRAE Guidelines. These settings are necessary to avoid overheating, condensation, and hardware corrosion. Consistent environmental conditions are maintained even during individual unit maintenance thanks to the use of N+1 redundant Precision Air Conditioning (PAC) units.

4. **Telecommunication and Connectivity**
   In this technical justification, telecommunications analysis ensured "the connection availability" through physical path redundancy. By utilizing two diverse entry points for carrier networks and automatic failover mechanisms between two or "multiple" different internet service providers (ISPs), XYZ University may mitigate the risk of a single point of failure. This setup guarantees the 99.982% uptime required for continuous access to the critical academic services.

As IT Asset Management and Lifecycle Thresholds, The formulation of this technical justification incorporates the End of Support Life (EoSL) metrics as a systematic framework to guide future operational audits of electronic and IT devices within the data center, forming a key component of XYZ University's IT Asset Management strategy; within this framework, asset conditions are classified into three lifecycle-based operational states, namely: (1) a normal operational state for devices with an age of up to 5 years, indicating optimal functionality and reliability; (2) a wary operational state for devices aged more than 5 years up to 10 years, where increased monitoring and preventive actions are required due to potential performance degradation; and (3) an unfit operational state for devices exceeding 10 years of age, which are associated with a high risk of failure and therefore necessitate mandatory replacement to ensure service continuity and system resilience.

The robustness of the technical justification was verified through a structured validation phase. To complete the technical justification draft, a Focus Group Discussion (FGD) with the IT Academic Support Unit was conducted on May 13th, 2025. On June 12th, 2025, a disaster scenario simulation was conducted after the draft was prepared to test the recovery time due to server disruptions, in addition to recording real incidents/disasters that had occurred within the last 1 year (including around of the time of the disaster scenario simulation or on June 12th, 2025). The results confirmed that the infrastructure designed according to this justification could meet the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) targets presented in Table 2.

Table 2. Recovery Performance Targets for XYZ University's IT Services

IT Service Category	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)
SIAKAD (Academic Information Systems)	≤ 2 hours	≤ 15 minutes
LMS (Learning Management System)	≤ 2 hours	≤ 15 minutes
Research and Final Project Repositories	≤ 4 hours	≤ 1 hour
General Administrative Services	≤ 6 hours	≤ 3 hours

5. Conclusion

Developing the Tier-3 XYZ University's data center is a strategic institutional requirement that tackles the substantial dependence of modern higher education on strong IT infrastructure. The comprehensive technical explanation of this research effectively addressed the systemic flaws and "single points of failure" in the institution's historical infrastructure. The results confirm that 99.982% uptime requires a methodical integration of international engineering references/standards (i.e., ANSI/TIA-942 and ASHRAE Guidelines) and national standard (SNI 8799) into institutional governance. This study established essential requirements for sub-1-ohm grounding systems, 500 kVA backup power, and N+1 redundancy, paving the way for eliminating the disturbances that have hampered fundamental academic goals.

The formalization of these technical justifications through the Rector's Decree provides the necessary governance framework for long-term success, signaling a strategic shift from reactive maintenance to proactive digital resilience. This policy integration ensures that XYZ University's digital heartbeat is protected by a synergy of technical engineering and administrative authority, establishing this study as the mandatory reference for ongoing disaster recovery and institutional continuity. Ultimately, the proposed architecture safeguards the productivity of the entire academic community and serves as a vital role model for partner universities in Indonesia, illustrating how high-availability infrastructure can be adapted to elevate the standards of higher education digital governance.

The physical implementation phase, which aims to realize a complete Tier-3 facility inside the university setting, is put in motion by the successful creation of this technical rationale. By 2034, the transition to a green data center will be given the greatest attention, with an emphasis on lowering Power Usage Effectiveness (PUE) via energy-efficient IT loads and sustainable cooling technologies. The research team also wants to further institutionalize information security and business continuity management systems by pursuing complete ISO 27001 and ISO 22301 certifications. To guarantee that XYZ University's digital infrastructure is robust against the changing landscape of global technology hazards, ongoing monitoring and recurring IT infrastructure audits based on the defined End of Support Life (EoSL) metrics will be carried out.

Acknowledgment

The authors are grateful to XYZ University for supporting this study through the Internal Research Grant scheme. We also wish to thank XYZ University's IT Academic Support Unit for their technical expertise and collaboration. As a pilot project, this study aimed to be a role model for technical justification frameworks for our partner universities within this collaborative initiative.

References

[1] P. D. A. S. Prabowo *et al*., “Technical Justification for the Development of Bank of XYZ Province’s Data Center,” in *Proceedings of the 5th Borneo International Conference*, Balikpapan, Indonesia: SCITEPRESS - Science and Technology Publications, 2025, pp. 33–39. doi: 10.5220/0013224500004605.

[2] TIA, *ANSI/TIA-942: Telecommunications Infrastructure Standard for Data Centers*. Arlington, 2005.

[3] BSN, *Indonesian National Standard (SNI) 8799-1:2023 – Information Technology – Data Center – Part 1: Technical Specifications for Data Centers*. Jakarta, ICS 35.020, 2023. [Online]. Available: www.bsn.go.id

[4] BSN, *Indonesian National Standard (SNI) 8799-2:2023 – Information Technology – Data Center – Part 2: Data Center Management System*. Jakarta, ICS 35.020, 2023. [Online]. Available: www.bsn.go.id

[5] F. G. F. Tabosa, D. A. da Silva, R. T. de Sousa, F. E. G. de Deus, and R. R. Nunes, “Risk Factors that Influence a Data Center Infrastructure through the TEMAC Method,” in *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)*, IEEE, Jun. 2021, pp. 1–6. doi: 10.23919/CISTI52073.2021.9476286.

[6] J. F. Andry, L. Liliana, H. Tannady, and A. S. Arief, “Data Centre Risk Analysis Using ISO 31000:2009 Framework,” in *Journal of Physics: Conference Series*, Institute of Physics, 2022. doi: 10.1088/1742-6596/2394/1/012032.

[7] ISO, *ISO/IEC 27001:2022 – Information Security Management Systems – Requirements*. Geneva, 2022.

[8] ISO, *ISO 31000:2018 – Risk Management*. Geneva, 2018.

[9] ISO, *ISO 27005:2022 – Information Security, Cybersecurity and Privacy Protection – Guidance on Managing Information Security Risks*. Geneva, Oct. 2022. [Online]. Available: www.iso.org

[10] AXELOS, *ITIL® Foundation: ITIL 4 Edition*. London: The Stationery Office, 2019.

[11] Project Management Institute, *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) and the Standard for Project Management*. Newtown Square, PA, USA: Project Management Institute, Inc., 2021.

[12] P. Gregory, *IT Disaster Recovery Planning for Dummies*. Indianapolis: Wiley Publishing, Inc., 2008.

[13] H. Taylor, *The Edge Data Center: Building the Connected Future*, 1st ed. Business Expert Press, 2023.

[14] H. Geng *et al*., *Data Center Handbook*, 1st ed. Wiley, 2021. doi: 10.1002/9781119597537.

[15] K. Jayaswal, *Administering Data Centers: Servers, Storage, and Voice over IP*. Indianapolis: Wiley Publishing, Inc., 2006.

[16] NFPA, *NFPA 110: Standard for Emergency and Standby Power Systems*, 2025.

[17] ISO, *ISO/IEC 27031:2011 – Cybersecurity – Information and Communication Technology Readiness for Business Continuity*. Geneva, 2011. [Online]. Available: https://standards.iteh.ai/catalog/standards/sist/c6b39744-5965-4b7b-a3f8-

[18] M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, and D. Lynes, “Contingency Planning Guide for Federal Information Systems,” National Institute of Standards and Technology, Gaithersburg, MD, USA, May 2010. doi: 10.6028/NIST.SP.800-34r1.

[19] NFPA, *NFPA 76: Standard for the Fire Protection of Telecommunications Facilities*, 2020.

[20] NFPA, *NFPA 75: Standard for the Fire Protection of Information Technology Equipment*, 2020.

[21] NFPA, *NFPA 72: National Fire Alarm and Signaling Code*, 2019.

[22] ISO, *ISO/IEC 27001:2022 – Information Security Management Systems*. Geneva, 2022.

[23] ASHRAE, *2021 ASHRAE Handbook: Fundamentals*, 2021.

[24] BSN, *General Requirements for Electrical Installations (PUIL) 2020 – Part 1: Introduction, Fundamental Principles, and Definitions*, SNI 0225-1:2020, Nov. 2020.

[25] OJK RI, *Financial Services Authority Regulation No. 38/POJK.03/2016 on Risk Management Implementation in the Use of Information Technology by Commercial Banks*. Indonesia, 2016.

[26] OJK RI, *Financial Services Authority Regulation No. 18/POJK.03/2016 on Risk Management Implementation for Commercial Banks*. Indonesia, 2016.

[27] OJK RI, *Financial Services Authority Regulation No. 13/POJK.03/2020 on Amendments to Regulation No. 38/POJK.03/2016*. Indonesia, 2020.

[28] N. M. V. A. Suryanti, I. N. Suweden, and I. W. A. Wijaya, “Design of a Tier 3 Standard Data Center Electrical System in Banking,” *Jurnal SPEKTRUM*, vol. 10, no. 4, pp. 357–364, 2023.
[29] Sunarno, *Advanced Mechanical Electrical Engineering*, 1st ed. Yogyakarta: Andi Publisher, 2006.
[30] Sunarno, *Mechanical Electrical Engineering*, 1st ed. Yogyakarta: Andi Publisher, 2005.
[31] Z. Xie, Y. Yang, and S. Lee, “Data Center Based on Cloud Computing Technology,” *International Journal of Informatics and Information Systems*, vol. 6, no. 1, pp. 31–37, 2023.
[32] X. Li, M. Li, Y. Zhang, Z. Han, and S. Wang, “Rack-Level Cooling Technologies for Data Centers – A Comprehensive Review,” Elsevier Ltd., Aug. 2024. doi: 10.1016/j.jobe.2024.109535.
[33] Q. Zhang *et al*., “A Survey on Data Center Cooling Systems: Technology, Power Consumption Modeling and Control Strategy Optimization,” *Journal of Systems Architecture*, vol. 119, p. 102253, Oct. 2021. doi: 10.1016/J.SYSARC.2021.102253.
[34] F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, “The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector,” *Sustainability*, vol. 15, no. 7, Apr. 2023. doi: 10.3390/su15075828.
[35] Syihabuddin, Y. Suryanto, and M. Salman, “Risk Management in Data Centers Using ISO 31000: Case Study XYZ Agency,” in *Proceedings of the 1st STEEEM*, 2019, pp. 341–352.
[36] M. Levy, “A Novel Framework for Data Center Risk Assessment,” in *2020 11th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, IEEE, Oct. 2020, pp. 0148–0154. doi: 10.1109/UEMCON51285.2020.9298072.
[37] Shammugam *et al*., “Information Security Threats Encountered by Malaysian Public Sector Data Centers,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 3, pp. 1820–1829, Mar. 2021. doi: 10.11591/ijeecs.v21.i3.pp1820-1829.
[38] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, “The ISO/IEC 27001 Information Security Management Standard: Literature Review and Theory-Based Research Agenda,” *TQM Journal*, vol. 33, no. 7, pp. 76–105, Mar. 2021. doi: 10.1108/TQM-09-2020-0202.
[39] S. Smernate, “Development of Information Security Management Systems under ISO/IEC 27001:2013 Standard: Case Study of Ministry of Public Health Internet Data Center,” *Journal of Health Science*, vol. 28, no. 1, pp. 117–131, 2019.
[40] Benyamin, M. Mualim, and E. P. Duarte, “Information Security Assessment of Yaza Agency Data Center to Prevent Cyber Threats in Enhancing Defense,” *Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI)*, vol. 6, no. 3, pp. 180–190, 2023.
[41] B. Barafort, A. L. Mesquida, and A. Mas, “Integrated Risk Management Process Assessment Model for IT Organizations Based on ISO 31000 in an ISO Multi-Standards Context,” *Computer Standards & Interfaces*, vol. 60, pp. 57–66, Nov. 2018. doi: 10.1016/J.CSI.2018.04.010.
[42] G. Beuchelt, “Information Technology Security Management,” in *Computer and Information Security Handbook*, pp. 475–508, Jan. 2025. doi: 10.1016/B978-0-443-13223-0.00027-8.
[43] Razikin and B. Soewito, “Cybersecurity Decision Support Model for Designing Information Technology Security Systems Based on Risk Analysis and Cybersecurity Framework,” *Egyptian Informatics Journal*, vol. 23, no. 3, pp. 383–404, Sep. 2022. doi: 10.1016/J.EIJ.2022.03.001.
[44] F. Abdullayeva, “Cyber Resilience and Cybersecurity Issues of Intelligent Cloud Computing Systems,” *Results in Control and Optimization*, vol. 12, p. 100268, Sep. 2023. doi: 10.1016/J.RICO.2023.100268.
[45] S. Acharya, A. A. Khan, and T. Päivärinta, “Interoperability Levels and Challenges of Digital Twins in Cyber–Physical Systems,” *Journal of Industrial Information Integration*, vol. 42, p. 100714, Nov. 2024. doi: 10.1016/J.JII.2024.100714.
[46] Gordon and G. Salazar-Chacon, “DRP Analysis: Service Outage in Data Center due to Power Failures,” in *2020 IEEE 11th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, IEEE, Nov. 2020, pp. 182–187. doi: 10.1109/IEMCON51383.2020.9284920.