Vol 13 No. 1, 2025

Jurnal Komputasi

Leveraging Cloud Computing for Network Infrastructure Disaster Mitigation and Recovery (A Case Study at STIKI Malang)

[1)] Wahyu Andika Pratama, [2,*)] Koko Wahyu Prasetyo

[1] Department of Informatics, Universitas Bhinneka Nusantara, Malang, Indonesia
[2] Department of Information Systems, Universitas Bhinneka Nusantara, Malang, Indonesia

Abstract *— Disasters are unpredictable and destructive events that can severely impact information technology services. This study develops a disaster recovery plan focusing on leveraging cloud computing to enhance disaster mitigation and recovery for network infrastructure. Specifically, it examines critical information system services and network infrastructure at STIKI Malang. Utilizing Google Cloud Platform, the study proposes a novel network topology and disaster recovery procedures, excluding budgetary and insurance considerations. The research outputs include a cloud-based network topology model and a comprehensive disaster recovery procedure. These are designed to minimize service disruptions and incorporate an alert system for responding disturbances on information system applications. Additionally, the study provides a risk analysis and preventive measures, offering operational guidelines to mitigate disaster impacts effectively. The findings aim to enhance resilience and ensure continuity of critical services, providing a valuable framework for institutions facing similar challenges. This research underscores the transformative potential of cloud computing in disaster management, offering strategic insights into integrating cloud solutions for robust network infrastructure resilience.*

Keywords: computer network; cloud computing; disaster recovery; IT infrastructure; risk mitigation

** Corresponding author :*
Koko Wahyu Prasetyo
Universitas Bhinneka Nusantara, Malang, Indonesia
Email: koko@ubhinus.ac.id

1. INTRODUCTION

Disasters, whether natural or human-made, pose significant risks to the operational continuity of organizations, particularly those reliant on information systems. Educational institutions like STIKI Malang are especially vulnerable due to their heavy dependence on IT services, such as academic platforms, administrative databases, and learning management systems. These systems are critical to maintaining academic operations, and their disruption can lead to financial losses, reputational damage, and compromised educational delivery [1], [2]. Consequently, robust disaster recovery (DR) planning has become a strategic necessity to safeguard academic continuity and institutional resilience.

Cloud computing has emerged as a transformative solution for modernizing DR strategies. By leveraging its scalability, flexibility, and cost-efficiency, organizations can create resilient systems capable of withstanding disruptions [3], [4]. Cloud platforms, such as Google Cloud, provide tools for automated failovers, real-time backups, and dynamic resource allocation, making them particularly valuable for institutions with constrained resources [5]. Moreover, integrating cloud-based DR solutions with established frameworks like NIST SP 800-34 offers a systematic approach to risk assessment, business impact analysis (BIA), and recovery strategy development [6], [7]. These advancements underscore the potential of cloud technologies to revolutionize disaster recovery in resource-constrained environments.

Despite these advantages, implementing effective DR strategies presents significant challenges. The diversity of disasters—ranging from cyberattacks to natural catastrophes—requires tailored solutions to address specific risks [7]–[9]. Financial constraints often hinder educational institutions from adopting advanced DR technologies and conducting adequate personnel training [1], [10]. Traditional DR methods, such as hot and cold sites or tape backups, remain costly and time-consuming to deploy, particularly for institutions with limited IT budgets [4]. Designing cost-effective DR plans that balance recovery time objectives (RTOs), costs, and data reliability is a persistent challenge [11].

Higher education institutions face unique challenges in disaster recovery due to their reliance on IT systems for critical operations like academic scheduling, e-learning, and financial management. Research conducted at a private university highlights the importance of adopting ISO/IEC 24762:2008 standards, which emphasize risk identification, BIA, and recovery strategies tailored to higher education environments [12]. Similarly, the implementation of NIST SP 800-34-based DR plans at another university demonstrated the role of structured frameworks in mitigating risks from natural disasters and cyberattacks, ensuring minimal downtime for critical services such as e-learning platforms [13].

The growing sophistication of cyber threats, including ransomware and insider attacks, further compounds these challenges. These threats are exacerbated by insufficient preparedness in managing private cloud systems and internal misuse [14]. Additionally, existing frameworks often fail to address localized needs, such as compliance with national standards like Indonesia's SNI 8799, which are critical for ensuring operational alignment and resilience [6], [15].

Cloud computing offers transformative opportunities to address these challenges. By enabling continuous backups, real-time monitoring, and automated recovery processes, cloud-based solutions reduce downtime and enhance system resilience [3]. Features such as asynchronous data replication and multi-region redundancy ensure data integrity even during large-scale disruptions [4], [16]. Additionally, integrating cloud platforms with frameworks like NIST SP 800-34 allows organizations to systematically identify risks, prioritize assets, and implement effective recovery strategies [17]. These solutions are especially advantageous for educational and governmental contexts, where resource optimization is essential [18], [19].

Recent studies underscore the impact of combining cloud technologies with standardized DR frameworks. Frameworks like NIST SP 800-34 have been widely adopted for their structured approach, which includes BIA, risk prioritization, and contingency planning [8], [10]. For resource-constrained institutions, these frameworks provide a roadmap for systematic disaster management while ensuring compliance with regional standards [7]. Case studies demonstrate how combining local standards, such as Indonesia's SNI 8799, with cloud-based solutions enhances operational resilience and cost efficiency [15].

This study aims to develop a comprehensive cloud-based DR plan tailored to the specific needs of STIKI Malang. The objectives are as follows:

a) Performing assessment on current IT infrastructure
b) Designing a cloud-based network topology model to enhance disaster resilience
c) Conducting a risk analysis to identify vulnerabilities and implement preventive measures

By addressing the unique challenges faced by educational institutions, this research contributes to the growing body of knowledge on DR planning. The study offers practical guidelines for achieving scalable disaster recovery solutions by utilizing cloud technologies in the education sector.

2. METHOD

This study employs a comprehensive methodology to develop a cloud-based disaster recovery plan (DRP) tailored to the specific needs of STIKI Malang. The methodology integrates systematic research

processes and practical implementation steps to ensure robust and applicable outcomes. The key steps can be seen in Figure 1.

Figure 1. Research methodology

This study adopts a comprehensive methodology to design a cloud-based disaster recovery plan (DRP) tailored to the specific needs of STIKI Malang. The process begins with an extensive literature review to establish a foundational understanding of disaster recovery frameworks, cloud-based solutions, and best practices. Case studies from educational institutions and government organizations provide practical insights into successful DR implementations, offering valuable benchmarks for this study.

Building on the literature review, primary data is collected from STIKI Malang to assess the current state of its IT infrastructure and disaster recovery preparedness. Interviews and focus group discussions with IT staff reveal workflows, challenges, and existing recovery practices. This qualitative data is supplemented with a review of internal documentation, including policies, and assets identification, to provide a complete perspective on system performance. Observational and document studies further improve the dataset by offering real-time insights into the institution's IT operations and identifying vulnerabilities. The collected data is analyzed to identify critical challenges and gaps in STIKI Malang's disaster recovery capabilities. Key risks are prioritized based on their potential impact on academic and administrative continuity.

A detailed evaluation of STIKI Malang's IT infrastructure follows, focusing on the strengths, weaknesses, and opportunities for improvement. The network topology is mapped to identify single points of failure and areas where redundancy can be introduced. The analysis also examines data management systems, evaluating the adequacy of backup and recovery mechanisms. Critical applications are reviewed to determine their dependencies and prioritization for recovery, while hardware and software configurations are assessed to ensure compatibility with cloud-based solutions.

Using insights from the preceding stages, a tailored DRP is developed for STIKI Malang. This plan includes recovery procedures for various disaster scenarios, such as hardware failure, cyberattacks, and natural disasters, ensuring comprehensive coverage of potential risks. The proposed DRP incorporates a cloud-based network topology designed to provide resilience and high availability. To validate the proposed DRP and ensure its robustness, a qualitative risk analysis is conducted. This analysis identifies potential disaster scenarios and evaluates their likelihood and impact using a risk matrix. Risks are categorized into high, medium, and low priority, enabling the development of targeted mitigation strategies.

3. RESULT AND DISCUSSION

This section presents the outcomes of the study, reflecting the systematic methodology employed to develop a disaster recovery plan (DRP) for STIKI Malang. The analysis of the institution's IT infrastructure revealed key vulnerabilities, such as single points of failure and inadequate backup processes, which informed the design of a robust, cloud-based DRP. Insights from the qualitative risk analysis further highlighted high-priority risks and shaped targeted mitigation strategies to enhance resilience.

3.1. Analysis of Current IT Infrastructure

The IT assets identification reveals a diverse range of assets critical to its academic and administrative operations. The institution relies on several servers to support its key systems, including web application

servers, and web hosting servers for institutional and unit-specific websites. Additionally, the database server manages essential data storage, while the FTP file server facilitates file transfers across systems. The network infrastructure supporting these systems includes advanced routing and switching hardware. Key components include some Routerboard models and cloud switch devices. These findings are presented in Table 1.

Table 1. List of identified IT assets

Asset Category	Identified Assets
Server	eBelajar LMS web server
	SAKTI web app server
	SIAKAD web app server
	SISTER web app server
	SIMONET web app server
	STIKI web hosting server
	Unit web hosting server
	PMB web app server
	Database server
	FTP file server
Network router	Routerboard CCR1036
	Routerboard RB1100HX2
	Routerboard RB450
	Hex PoE ethernet router
Network switch	CRS125 cloud switch

As shown in Table 2, STIKI Malang's IT ecosystem consists of various applications tailored to support both academic and administrative functions. The eBelajar LMS is a cornerstone platform utilized by faculty, staff, and students to facilitate e-learning and resource sharing. Complementing this are the SAKTI and SIAKAD systems, which manage student and faculty academic activities, respectively. Additionally, the PMB admission system, along with the institution's main and unit-specific websites, provides essential communication and outreach services, supporting both prospective students and internal stakeholders.

Table 2. List of identified IT business apps

Business Apps	User			Learning-related	Administrative-related
	Faculty	Staff	Student		
STIKI institution website		x	x		x
PMB admission sytem		x	x		x
Unit-specific websites		x	x		x
eBelajar LMS	x	x	x	x	
SAKTI student academic system	x		x	x	
SIAKAD faculty academic system	x	x		x	
SISTER academic resource system	x	x			x
SIMONET network monitoring system		x			x

Table 2 also highlights the inclusion of administrative tools like the SISTER academic resource system, which grants students and staff access to critical academic resources, and the SIMONET network monitoring system, designed to assist IT staff in managing and maintaining network infrastructure. While these systems are integral to STIKI Malang's day-to-day operations, the analysis underscores the critical need for robust disaster recovery measures to ensure their availability during disruptive events.

STIKI Malang's current backup strategy utilizes RAID 0, which improves read and write speeds and increases storage capacity by stripping data across multiple disks. However, the lack of redundancy in RAID 0 makes it vulnerable to data loss in the event of disk failure. Furthermore, SIMONET emergency alert system monitors device status and connectivity, sending notifications via email and Telegram to the network infrastructure team when devices go offline. While functional for basic monitoring, the system is limited to device availability and does not cover broader disaster scenarios.

The network topology at STIKI Malang, as shown in Figure 2, features a hierarchical structure with a main router connected to two ISPs for internet redundancy. The main router links to a central switch, distributing traffic to two Proxmox servers that host critical applications. While this setup ensures efficient traffic management, it introduces single points of failure at the main router and switch, posing risks to overall connectivity.

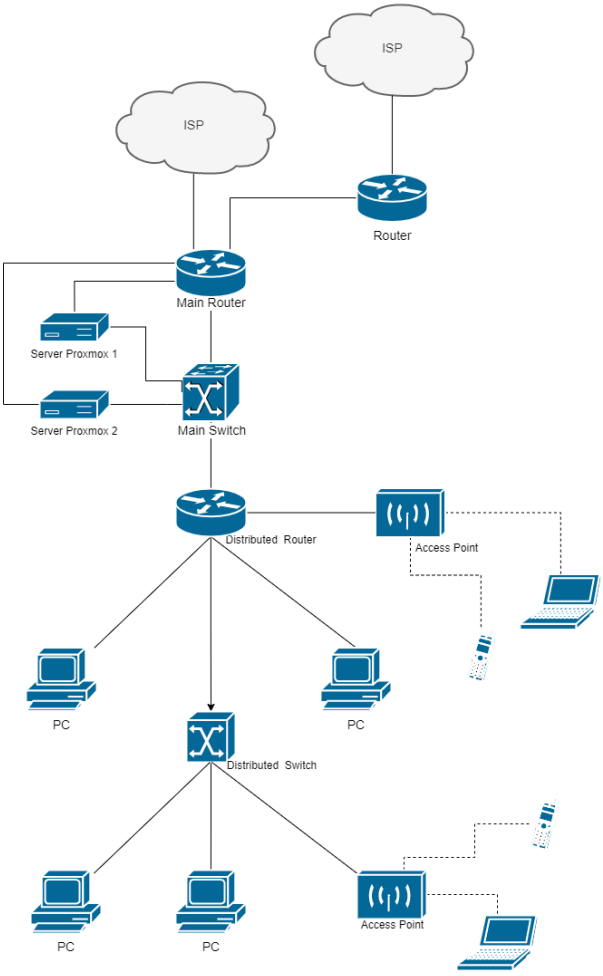

Figure 2. Current IT network topology

Beyond the core, distributed routers and switches extend connectivity to endpoint devices, including PCs and access points for wireless access. Although the distributed design ensures wide coverage, its reliance on the central infrastructure highlights the need for redundancy. Enhancing fault tolerance at the core network level, such as with backup routers and switches, is essential to maintaining reliability and mitigating disruptions during disasters.

Interviews with the IT Infrastructure team highlight critical dependencies on priority services such as E-Belajar, SAKTI, SIAKAD, and the institution's primary website. Disruptions to these services could halt academic and administrative operations.. The team also faces challenges in monitoring the Proxmox servers, limiting their ability to detect and respond to failures promptly. Developing a comprehensive DRP and enhanced network topology will help address these issues, improve system resilience, and minimize the impact of unexpected disasters.

3.2. Proposed Cloud-based IT Topology

The proposed network topology enhances resilience by integrating physical and cloud-based assets for improved reliability and disaster recovery. It includes network routers and switches for on-premises connectivity, Google Compute Engine for hosting critical applications, and Google Cloud Storage for secure data management. This strategic classification optimizes performance, fault tolerance, and recovery efficiency. Table 3 outlines the asset distribution in the proposed infrastructure.

Table 3. Proposed IT assets and services

Asset Category	Proposed Asset List
Network router	Routerboard CCR1036
	Routerboard RB1100HX2
	Routerboard RB450
	Hex PoE ethernet router
Network switch	CRS125 cloud switch
Google Compute Engine	Cloud-hosted router
	P1 CE: SAKTI, SIAKAD, SISTER
	P2 CE: eBelajar
	P3 CE: PMB, websites, SIMONET
	Database CE
Google Cloud Storage	File storage service

The proposed infrastructure categorizes assets into network hardware and cloud services to enhance performance and resilience. Network routers and switches ensure stable on-premises connectivity, while Google Compute Engine hosts critical web applications as collections of virtual machines, including academic systems in P1 Engine and administrative systems in P3 Engine. Google Cloud Storage provides secure file storage, supporting data redundancy and accessibility. This hybrid approach strengthens disaster recovery capabilities and ensures service continuity.

The proposed cloud-based topology, as illustrated in Figure 3, enhances resilience by integrating Google Compute Engine instances (P1, P2, and P3) with the existing on-premises infrastructure. By hosting critical applications, database, and storage services in the cloud, this design reduces reliance on local servers, minimizing the risk of data loss and service disruptions caused by hardware failures or natural disasters. The cloud-hosted router ensures seamless connectivity between cloud resources and on-premises systems, providing a scalable and secure environment for essential services.

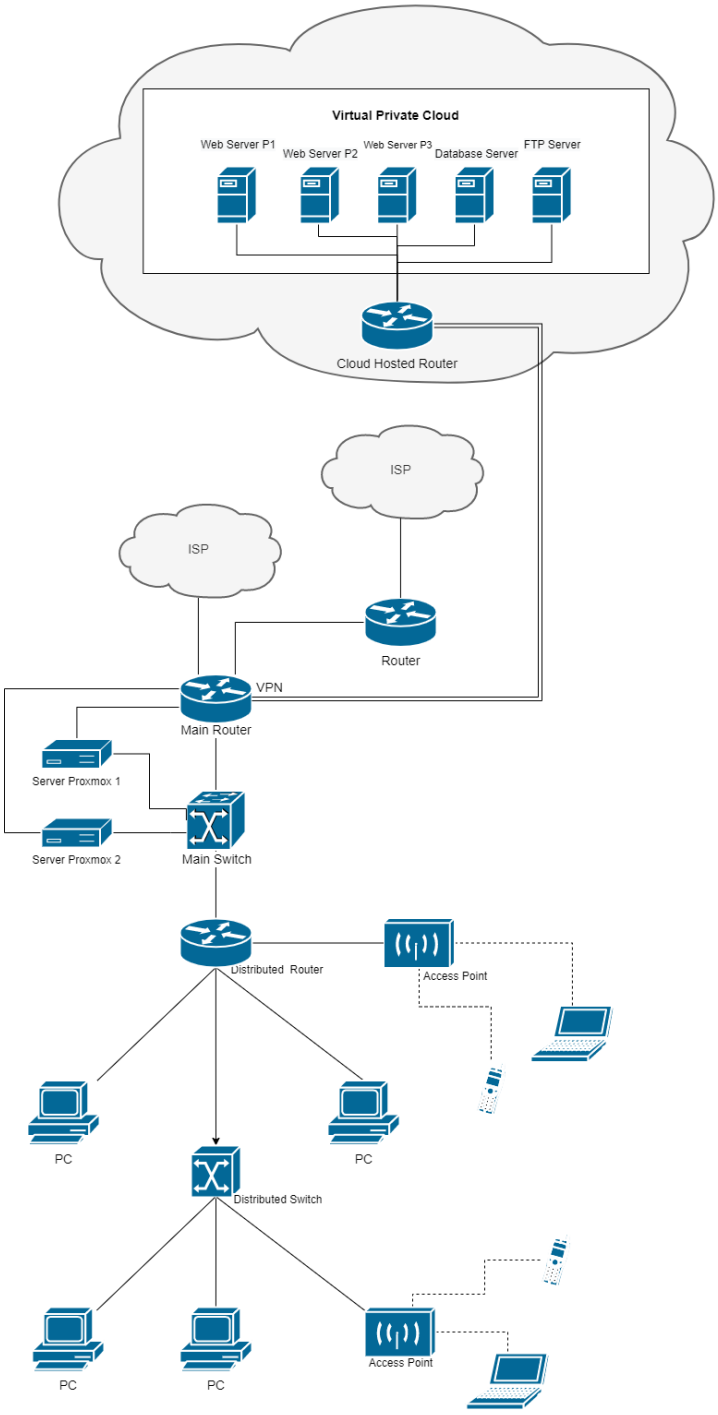

Figure 3. Proposed cloud-based IT network topology

This hybrid model improves fault tolerance and redundancy by distributing workloads between on-premises Proxmox servers and cloud-hosted instances and database engine. In the event of local server failure, critical applications can continue running from the cloud, ensuring uninterrupted access to academic and administrative systems. Additionally, the VPN connection between the main router and cloud infrastructure secures data transmissions, reducing vulnerabilities associated with traditional network architectures.

The inclusion of distributed routing and switching further strengthens network resilience by preventing single points of failure. The main and distributed routers work together to optimize traffic flow, while

multiple access points ensure robust wireless coverage across campus. This design supports scalability and disaster recovery, allowing STIKI Malang to maintain operational continuity even in unexpected scenarios. By leveraging cloud computing, the institution gains a cost-effective, flexible, and highly available infrastructure that is better equipped to handle future challenges.

3.3. Risk Identification and Response

A risk analysis was conducted to identify potential threats to STIKI Malang's IT infrastructure and assess their impact on operational continuity. The analysis considers various risks, including hardware failures, network disruptions, and environmental factors. Each risk is evaluated based on its severity, probability of occurrence, and necessary mitigation strategies to minimize disruptions. Table 4 presents the identified risks along with their respective responses.

Table 4. Identified risks and mitigation responses

ID	Potential Risk	Impact	Probability	Mitigation Response	Risk Level
R1	Electrical Disturbance	Severe	Frequent	Use equipment that stabilizes electrical currents.	High (H)
R2	Fire	Very Severe	Rare	Install fire extinguishers (APAR) in accessible locations.	Medium (M)
R3	ISP Network Issues	Moderate	Occasional	Implement load balancing and failover mechanisms; monitor ISP performance and enforce SLAs.	Medium (M)
R4	Low Human Resource Capacity	Moderate	Occasional	Provide training on network infrastructure.	Medium (M)
R5	Cyber Attacks	Low	Rare	Implement multiple layers of security on devices.	Low (L)
R6	Animal-Related Damage	Minor	Rare	Use protective covers for equipment.	Low (L)

The risk assessment highlights electrical disturbances as the most frequent and severe threat to STIKI Malang's IT infrastructure. As previous studies have emphasized, power stability is crucial in maintaining uninterrupted IT services, particularly in educational institutions that depend on digital platforms [1], [2]. Power fluctuations can lead to hardware failure and data corruption, disrupting critical applications such as E-Belajar, SAKTI, and SIAKAD. While the current mitigation strategy involves electrical stabilizers, studies suggest that implementing UPS and backup generators can significantly reduce downtime and mitigate risks. Additionally, real-time power monitoring systems could further enhance preparedness, aligning with the recommendations from disaster recovery frameworks such as NIST SP 800-34 [6].

ISP network issues present a moderate yet disruptive risk, as educational institutions depend heavily on stable internet access for e-learning and administrative operations. Previous research emphasizes the importance of redundant network architectures to mitigate disruptions caused by ISP failures [7]. The proposed load balancing and failover mechanisms, combined with strict Service Level Agreement (SLA) enforcement, align with best practices for network resilience [8]. Further improvements, such as Software-Defined Wide Area Networks (SD-WAN), could enable dynamic switching between multiple ISPs, ensuring uninterrupted connectivity [15].

Previous studies on cloud security frameworks emphasize that layered security approaches, including intrusion detection systems (IDS), real-time threat monitoring, and periodic penetration testing, are

essential for mitigating cyber risks [14]. The risk register recommends structured training programs to address skill gaps, a solution supported by findings that ongoing cybersecurity education significantly reduces vulnerabilities in cloud environments [8]. Additionally, integrating access control policies and collaborating with external cybersecurity experts would strengthen STIKI Malang's disaster recovery strategy, ensuring compliance with national security standards like SNI 8799 [6].

By addressing these risks through a cloud-based disaster recovery plan, STIKI Malang can enhance operational resilience, ensuring continuity in academic and administrative services. The findings support prior research on hybrid disaster recovery models [5], which combine on-premises infrastructure with cloud-based redundancy to improve reliability and scalability. The proposed mitigation strategies align with industry best practices and provide a cost-effective, scalable model that can be adopted by other educational institutions facing similar challenges.

4. CONCLUSION

This study proposes a cloud-based disaster recovery plan (DRP) to enhance the resilience of STIKI Malang's IT infrastructure. The analysis identified key vulnerabilities, including reliance on critical services, limited backup mechanisms, and network monitoring challenges. Addressing these risks, the proposed DRP and cloud-based topology offer a scalable, fault-tolerant solution to ensure service continuity.

By integrating scalable cloud-hosted services, load balancing, and structured recovery procedures, the plan strengthens disaster preparedness and aligns with best practices. This framework not only meets STIKI Malang's needs but also serves as a model for other educational institutions seeking to improve IT resilience. Ongoing evaluation, staff training, and policy updates will be essential for sustaining its effectiveness in an evolving digital landscape.

REFERENCES

[1] I. G. T. Isa, "Implementasi Pendekatan Kerangka Kerja NIST 800-34 dalam Perancangan Disaster Recovery Plan pada Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi," *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, vol. 15, no. 2, Art. no. 2, Sep. 2020, doi: 10.30872/jim.v15i2.3724.

[2] S. W. Sari and K. Ramli, "Perancangan Disaster Recovery Plan Pada Pusat Data Dan Teknologi Informasi Komunikasi Instansi XYZ," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 11, no. 4, Art. no. 4, Aug. 2024, doi: 10.25126/jtiik.1148959.

[3] M. Z. Hasan, N. Sarwar, I. Alam, M. Z. Hussain, A. A. Siddiqui, and A. Irshad, "Data Recovery and Backup management: A Cloud Computing Impact," in *2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T)*, Bahawalpur, Pakistan: IEEE, Jan. 2023, pp. 1–6. doi: 10.1109/ICEST56843.2023.10138852.

[4] O. R. Arogundade, "Cloud vs Traditional Disaster Recovery Techniques : A Comparative Analysis," *INTERNATIONAL ADVANCED RESEARCH JOURNAL IN SCIENCE, ENGINEERING AND TECHNOLOGY*, vol. 10, no. 4, Apr. 2023, doi: 10.17148/IARJSET.2023.10430.

[5] O. Cheikhrouhou, A. Koubaa, and A. Zarrad, "A Cloud Based Disaster Management System," *Journal of Sensor and Actuator Networks*, vol. 9, no. 1, Art. no. 1, Mar. 2020, doi: 10.3390/jsan9010006.

[6] H. G. Afiansyah, S. U. Sunaringtyas, and A. Amiruddin, "Perancangan Rencana Pemulihan Bencana Menggunakan NIST SP 800-34 Rev 1, NIST SP 800-53 Rev 5 dan SNI 8799 (Studi Kasus: Unit TI XYZ)," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 10, no. 2, Art. no. 2, Apr. 2023, doi: 10.25126/jtiik.20231026507.

[7] I. E. Nurdin, "Development of an Integrated it Risk Management Framework for Electronic-Based Government Systems: A Case Study of The XYZ Ministry," *Indonesian Interdisciplinary Journal of Sharia Economics (IIJSE)*, vol. 7, no. 1, Art. no. 1, Jan. 2024, doi: 10.31538/iijse.v7i1.4322.

[8] E. D. Pamungkas, N. S. Fatonah, G. Firmansyah, and H. Akbar, "Disaster Recovery Plan Analysis Based on the NIST SP 800-34 Framework (Case Study: PT Wijaya Karya (Persero) Tbk.)," *Jurnal Indonesia Sosial Sains*, vol. 4, no. 09, pp. 936–947, Sep. 2023, doi: 10.59141/jiss.v4i09.879.

[9] L. Jiao, Y. Zhu, X. Huo, Y. Wu, and Y. Zhang, "Resilience assessment of metro stations against rainstorm disaster based on cloud model: a case study in Chongqing, China," *Nat Hazards*, vol. 116, no. 2, pp. 2311–2337, Mar. 2023, doi: 10.1007/s11069-022-05765-2.

[10] M. H. Alifian and D. Priharsari, "Penyusunan Disaster Recovery Plan (DRP) menggunakan framework NIST SP 800-34 (Studi Kasus pada Perusahaan IT Nasional)," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 5, no. 10, Art. no. 10, Oct. 2021.

[11] A. Z. Abualkishik, A. A. Alwan, and Y. Gulzar, "Disaster Recovery in Cloud Computing Systems: An Overview," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 11, no. 9, Art. no. 9, Aug. 2020, doi: 10.14569/IJACSA.2020.0110984.

[12] D. Y. Bernanda, Y. Charolina, O. Azhari, C. Pangrestu, and J. F. Andry, "IDENTIFICATION OF POTENTIAL AND PLANNING FOR DISASTER RECOVERY USING THE ISO/IEC 24762 STANDARD AT XYZ UNIVERSITY," *Jurnal Teknoinfo*, vol. 17, no. 1, Art. no. 1, Jan. 2023, doi: 10.33365/jti.v17i1.2295.

[13] A. Setyawan, Y. Giri Sucahyo, and A. Gandhi, "Design of Disaster Recovery Plan: State University in Indonesia," in *2020 Fifth International Conference on Informatics and Computing (ICIC)*, Gorontalo, Indonesia: IEEE, Nov. 2020, pp. 1–5. doi: 10.1109/ICIC50835.2020.9288543.

[14] Reza Febriana and Ahmad Luthfi, "Comparative Study of Cloud Forensic Investigation Using ADAM And NIST 800-86 Methods in Private Cloud Computing," *J. RESTI (Rekayasa Sist. Teknol. Inf.)*, vol. 7, no. 5, pp. 1097–1110, Oct. 2023, doi: 10.29207/resti.v7i5.5279.

[15] J. Chaidir and H. Haerofiatna, "Network Infrastructure Development in Serang District," *International Journal of Management Technology*, vol. 10, no. 1, Art. no. 1, Jun. 2023.

[16] E. Andrade and B. Nogueira, "Dependability evaluation of a disaster recovery solution for IoT infrastructures," *J Supercomput*, vol. 76, no. 3, pp. 1828–1849, Mar. 2020, doi: 10.1007/s11227-018-2290-0.

[17] D. Suhartono and K. N. Isnaini, "Strategi Recovery Plan Teknologi Informasi di Perguruan Tinggi Menggunakan Framework NIST SP 800-34," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 20, no. 2, Art. no. 2, May 2021, doi: 10.30812/matrik.v20i2.1097.

[18] D. Yuniarto, "Implementing Cloud Computing in Companies to Increase Business Efficiency," *Jurnal Info Sains : Informatika dan Sains*, vol. 13, no. 02, Art. no. 02, Nov. 2023.

[19] B. Baharuddin, D. Ampera, H. Febriasari, M. A. R. Sembiring, and A. Hamid, "Implementation of Cloud Computing System in Learning System Development in Engineering Education Study Program," *International Journal of Education in Mathematics, Science and Technology*, vol. 9, no. 4, Art. no. 4, Oct. 2021, doi: 10.46328/ijemst.2114.