TADWIN : Jurnal Ilmu Perpustakaan dan Informasi
Available online at: https://jurnal.radenfatah.ac.id/index.php
Vol. 6 No. 2, December 2025, pages: 154-168
Copyright ©2020, ISSN: 27232409 print/online 2774-8936
https://doi.org/10.19109/tadwin.v6i2.29864

Design of a Disaster Recovery Plan Document at the Daniel S. Lev Law Library

Dwi Fajar Saputra[1*], Fahmi Arya Muzakir[2], Kaira Naafila Zahra[3], Syifa Rizki Amalia[4], Shanata Zahwa Fitriana[5], Zhahiru Rafli Firmansyah[6], Muhammad Mizan Murazaki Sani[7]

[1234567]Universitas Pembangunan Nasional Veteran Jakarta, Indonesia
*Email correspondence: dwifajar@upnvj.ac.id

Information

Submited: 24-09-2025
Revised: 20-11-2025
Accepted: 04-12-2025

How to cite: Design of a Disaster Recovery Plan Document at Daniel S. Lev Law Library. (2025). *TADWIN: Jurnal Ilmu Perpustakaan dan Informasi*, 6 (2), 154-168. https://doi.org/10.19109/tadwin.v6i2.29864

DOI: doi.org/10.19109/tadwin.v6i2.29864

ABSTRACT

A Disaster Recovery Plan (DRP) should be tailored to an institution's specific needs and characteristics in order to maintain information service continuity amid potential vulnerabilities in the information system. A qualitative approach was used to collect data through observations, semi-structured interviews with the library director and IT staff, and internal documentation studies. The Daniel S. Lev Law Library uses various systems for daily operations and is highly dependent on five main information systems: Digilev, the Institutional Repository, Catalog Danlev, the Court Decisions System, and the Internal Archiving System. The analysis of critical information systems and potential risks was based on the NIST SP 800-34 Rev. 1 framework and the FIPS 199 guidelines. The results showed that Digilev and the Institutional Repository had the highest impact levels because they are directly related to academic research and accreditation requirements. Additionally, we conducted Recovery Time Objective (RTO) and Recovery Point Objective (RPO) identification to establish priorities for effective information system recovery strategies based on disruption scenarios such as server downtime, cyber threats, and natural disasters. These strategies include providing backups and backup servers, enhancing system security, training staff, and creating emergency plans for physical disasters. These results are all documented in a structured disaster recovery plan that serves as a technical guide and institutional regulation for anticipating and addressing issues that could disrupt the information system. It is hoped that this plan will enhance security and ensure the continuity of digital library services at the Daniel S. Lev Law Library.

Keywords: *Disaster Recovery Plan; Digital Library; Information System Risk; Service Continuity; NIST SP 800-34.*

1. INTRODUCTION

Information and technology systems (IS/IT) are now the main foundation in supporting library operations in the digital era (Onunka et al., 2023) . With this system, libraries are not only able to provide fast and efficient access to information, but also expand their services to all users online (Taherdoost, 2023) . In this case, information has transformed from a mere complement to a strategic asset whose continuity must be maintained (Ikenwe & Udem, 2022) . Therefore, various disruptions to information systems, whether from natural disasters, technical damage, cyber-attacks, or *human error*, have the potential to cause serious impacts on institutional operations and reputation (Beretas, 2024).

As libraries become increasingly dependent on digital technology, the need for information system risk management is becoming more urgent (Rahmani, 2025). Risk management not only includes identifying potential threats, but also assessing the vulnerability level of the technological infrastructure used by libraries (Dada et al., 2025). Without proper risk management, libraries are at risk of service disruptions that can hamper information retrieval, borrowing, and access to electronic databases (Garnett, 2021). This shows that investing in the security and sustainability of information systems is no longer just an option, but a necessity for libraries to continue to meet the expectations of modern users who demand unhindered access to information (Enakrire et al., 2024).

In addition, digital transformation also requires libraries to have infrastructure that is adaptive to technological developments (Onunka et al., 2023). The information system used must be able to integrate with various service platforms, such as online catalogs, digital repositories, journal databases, and web-based reference services (Revathi & Mohan, 2022). This integration not only facilitates operational activities but also enhances the user experience in accessing information (Di Sutam et al., 2024). However, the increasing complexity of system integration also increases the potential for disruption if not managed properly (Dekker et al., 2022). Therefore, libraries need to ensure that the implemented system has an adequate level of stability, security, and scalability to be able to cope with the dynamics of user needs and potential technological risks in the future (Oyedokun, 2025).

Various studies have emphasized the importance of institutional preparedness in facing these risks. For example, Nurul Afifah et al. (2019) in their research focusing on the design of *a Disaster Recovery Plan* (DRP) for the Purbalingga Regional Library, emphasized that DRP is a crucial instrument to ensure service continuity after a system disruption. This document contains procedures, policies, and recovery strategies designed to ensure that information systems can return to normal operation with minimal impact on users. However, the implementation of DRPs in various institutions in Indonesia, including libraries, is still minimal and has not been specifically tailored to the characteristics of each local institution (Nurul Afifah et al., 2019).

One such institution is the Daniel S. Lev Law Library, a legal library service unit under the Foundation for Legal Studies and Policy (YSHK). This library manages various important information systems such as Digilev (digital collection), Institutional Repository, Danlev *Catalog* (based on SLiMS), and internal archiving systems. In practice, this service faces various potential risks such as server damage, *malware* infection, and *human error* due to weak security systems (Magsi et al., 2025) . Based on the results of in-depth observations and interviews, it is known that until now the library does not have a formally and standardized DRP document.

This problem highlights the need to develop a *Disaster Recovery Plan* document that is specifically tailored to the infrastructure conditions, availability of human resources, and operational needs of the library (Dada et al., 2025) . Therefore, this study aims to design a DRP document whose scope is not limited to technical aspects but also integrates policy considerations and *recovery* practices that have been informally implemented. The preparation of this document will be based on the NIST SP 800-34 Rev. 1 framework and adapted to the actual conditions at the Daniel S. Lev Law Library, so that it can serve as a strategic guideline in dealing with various disruptions to information services.

2. RESEARCH METHOD

This research uses a qualitative approach with the aim of designing a *Disaster Recovery Plan* (DRP) document for the information system used at the Daniel S. Lev Law Library. This approach was chosen because it allows researchers to directly understand the actual conditions of the IS/IT infrastructure, library operational processes, and potential risks faced in the event of a disruption or disaster. The qualitative approach also allows for in-depth exploration of experiences and internal policies related to preparedness for system disruptions. According to Sugiyono (2022), the qualitative approach is used to study the natural conditions of an object, where the researcher is the key instrument (Sugiyono, 2022). The informant selection technique was carried out *purposively*, namely by selecting parties who have direct knowledge and responsibility for managing the library information system. In this case, the informants consisted of the Head of the Library and the Information Technology staff. Both were selected because they were considered to have the best understanding of the managerial and technical aspects of the existing information system.

This research was conducted during June 2025, starting from the preparation stage to the preparation of the final DRP document. The data collection period was carried out in the middle of the month. The data collection techniques used in this study included observation, interviews, and documentation studies. Observations were made by directly observing the condition of the IS/IT infrastructure, including hardware, software, networks, and ongoing operational procedures. Semi-structured interviews were conducted with the Head of the Library and IT personnel to gather information about past risks, disruption management policies, estimated system recovery times, and so on. Meanwhile, documentation studies were conducted by reviewing internal documents such as organizational structures, SOPs, library standards, and other supporting data relevant to DRP planning. To maintain data validity, this study applied source and method triangulation by comparing the results of interviews, field observations, and internal supporting documents. This step was taken to ensure the consistency and accuracy of the data before it was used in the analysis and DRP preparation process.

The data collected through observation, interviews, and documentation studies was analyzed with reference to the NIST Special Publication 800-34 Revision 1 framework. This framework was chosen because it provides clear and structured guidance in the preparation of *a Disaster Recovery Plan* (DRP). In addition, NIST SP 800-34 Rev. 1 is widely used as an international reference standard in information system recovery planning, so it is considered appropriate for the objectives of this study. The analysis was carried out systematically through several stages. The first stage was the identification of information system assets and services to determine the important components that support library operations. Next, a *risk assessment* was conducted to assess potential threats and vulnerabilities to existing IS/IT assets. After that, *a business impact analysis* was conducted to estimate the operational impact in the event of a system disruption. Based on the results of these analyses, a recovery strategy and contingency plan are developed, including system prioritization ( ), recovery procedures, and an estimate of the time required for recovery. The final stage involves documenting and compiling the DRP, which produces guidelines for information system recovery at the Daniel S. Lev Law Library. This approach allows the collected data to be mapped in a structured manner into the main elements needed in the compilation of *the Disaster Recovery Plan* (DRP) document.

3. RESULTS AND DISCUSSION

IS/IT Network Scheme

Within the framework of *Contingency Planning* NIST SP 800-34 Rev. 1 and *Control Business Continuity* SNI ISO/IEC 27001:2022 (specifically A.5.29 and A.17.1), organizations must ensure that IS/IT infrastructure is built redundantly and segmented to ensure service continuity during disruptions (NIST, 2010). The Daniel S. Lev Law Library has implemented a mixed infrastructure scheme consisting of two physical local servers, two virtual *cloud* servers on Google Cloud, and three *shared hosting* services. This scheme reflects a *hybrid infrastructure* approach that is adaptive to accessibility, flexibility, and cost efficiency needs, while still paying attention to relevant resilience and risk control aspects. *The cloud* is used for active and critical public services such as *repositories* and *e-learning*, while local servers are intended for systems with lower sensitivity or access frequency.

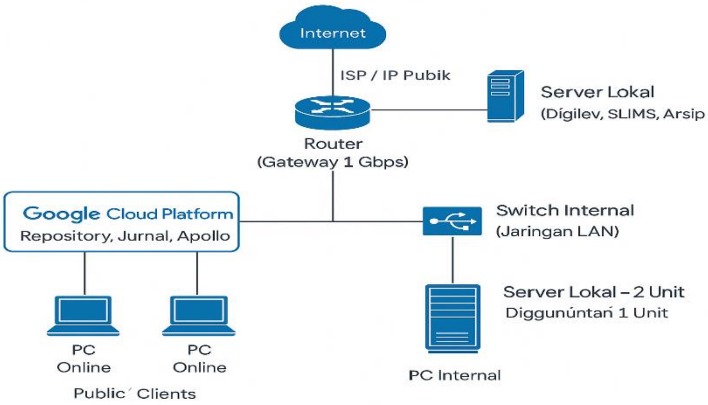

Figure 1. Local and *Cloud* Server Infrastructure Topology
(Local: CPU: 4vCPU, RAM: 16 GB, *Operating System*: Linux Debian/Ubuntu Server 64-bit and *Cloud*: Google Cloud Platform)

Daniel S. Lev Law Library Information System

The Daniel S. Lev Law Library utilizes several information systems that play an important role in the management of daily library services, both for internal and external needs. To provide a more structured overview of the information systems used, the following table is presented:

Table 1. Information System Service *Mapping*

No.	Information System	Service
1	Digilev	Digital collection management system for *e-books*, *e-papers*, *grey literature*, and *clippings* specifically for internal staff
2	Institutional Repository	A system for storing theses, scientific papers, and faculty research for accreditation purposes and public access.
3	Danlev *Catalog* (based on SLiMS)	Library catalog and collection recording service system, used for searching printed books.

4	Court Decisions	Provides a collection of Supreme Court decisions and jurisprudence that can only be accessed by internal staff
5	Internal Archiving System	An internal document archiving system that can only be accessed through the local area network (LAN) at the office.

Risk Assessment

Risk *assessment* is a systematic process that aims to identify, analyze, and reduce various potential risks that could disrupt operational continuity and the achievement of organizational goals (Balaji et al., 2024) . In this discussion, Table 2 presents a list of various real threats that may occur, complete with vulnerabilities, affected assets, and the consequences for organizational operations.

Meanwhile, Table 3 complements this analysis with a mapping of these threats. Specifically, the analysis uses a *qualitative risk assessment* method with a *Risk Matrix* approach, considering the level of relevance (*Likelihood of Relevance*), possibility (*Likelihood*), impact (*Impact*), and risk level (*Risk Level*). Through a combination of these two tables, institutions can obtain a more comprehensive picture of the potential risks they face and determine effective and strategic handling priorities.

Table 2. *Risk Assessment*

No	Threat	Occurring Threat	Vulnerability	Critical Assets	Consequences
1	Lightning	Lightning strikes can damage electrical or LAN systems and electronic devices	Lightning can cause damage to servers	Servers, electronic devices, LAN networks, library buildings	a. Cessation of operational activities b. Damage to electrical and LAN networks and electronic devices
2	Earthquakes	Can damage building infrastructure if it exceeds 5 on the Richter scale	The building can only withstand up to 5 on the Richter scale	Library buildings, physical collections, servers	a. Physical facility damage b. Library services disrupted
3	Fire	Fire caused by electrical short circuit or other causes	Flammable materials in every room and building	Book collection, reading room, staff room, library building	a. Loss of collection b. Interruption of library services and operations
4	Power outages	Loss of power or unstable voltage	Equipment requiring electricity not	Computers, office assets,	a. System-based service failure

			functioning normally	and office equipment	b. Potential equipment damage
5	Server Down	The server is damaged and cannot be accessed by users	Server damage	Library server, online catalog system	a. Borrowing services disrupted b. Unable to access OPAC and user data
6	Virus attack	Worms, malware, or viruses attack the system	Applications and OS have security vulnerabilities, emails are infected	Library information system, collection data	a. Loss of collection data or user information
7	Cyber Threat	*Hackers* exploit security holes to gain access	Weak passwords	Information, reputation	a. Leakage of confidential information b. Damage to reputation
8	Human error	Loss of data and information.	Data deletion, data entry errors.	Data and information on the Daniel S. Lev Law Library system and digital book assets	a. Computer malfunction, slow system performance, or system shutdown.
9	System Failure	System failures such as *server downtime*, *software crashes*, or system information failure at the library	Lack of data backup, absence of a recovery system, software not updated	Library servers, catalog databases, computer network , library information systems	a. Disruption of library services, loss of important data , user complaints, operational downtime
10	Human Deliberate	Theft of organizational assets without permission, both physical (e.g., hardware) and digital (data, files, important documents).	Absence of CCTV or physical surveillance in the server room.	Hardware such as laptops, external hard drives, servers. Or digital data such as: member databases, digital archives,	a. Loss of important data that cannot be recovered (if there is no backup). b. Leakage of sensitive information,

				financial documents.	such as member identities or research data. c. Damage to the institution's reputation due to perceived negligence in data protection.

Table 3. *Risk Assessment* Mapping

No.	Threat	Relevance	Probability	Impact	Risk
1	Data Leakage / Sensitive Information	C	T	ST	ST
2	Hacking	A	ST	ST	ST
3	Phishing	C	S	ST	T
4	Virus/Malware Infection	P	S	ST	T
5	Administrative Error	C	R	R	R
6	Procedural Error	P	S	T	S
7	Damaged Device	C	R	ST	P
8	Device Stolen	A	R	ST	S
9	Installation Failed	C	S	ST	S
10	Backup Failure	C	ST	T	T
11	Data Lost	C	T	ST	T
12	Damaged Data	C	R	T	T
13	Dwindling Resources	P	T	T	T
14	Internet Disruption	C	T	T	T
15	Blackout/Power Outage	C	T	S	R

16	Fire	P	R	ST	R
17	Earthquake	T	T	ST	T
18	Lightning	A	ST	ST	ST
19	System Failure	P	R	ST	S
20	Human Deliberate	P	T	ST	S

Description:

1. Relevance: C (*Confirmed*), A (*Anticipated*), P (*Possible*), R (*Rare*), T (*Typical*)
2. Likelihood: ST (Very High), T (High), S (Moderate), R (Low)
3. *Impact*: ST (Very High), T (High), S (Moderate), R (Low)
4. Risk: ST (Very High), T (High), S (Moderate), R (Low)

Business Impact Analysis **(BIA)**

Business Impact Analysis is an important step in preparing a *Disaster and Recovery Plan* document. BIA makes it easier for library managers to overcome operational impacts, organizational reputation, and possible data loss caused by disruptions, whether natural disasters, *cyber* attacks, or internal *human error*. BIA is carried out to identify important business processes and analyze the possible effects if a disaster or disruption affects information and technology (IS/IT) systems.

This process involves assessing the impact over time on human resources, products, services, and customers, and is essential for developing strategies to ensure business resilience. The BIA process includes identifying critical business functions, resources, acceptable downtime, and recovery objectives, which form the basis for emergency recovery and disaster recovery plans. This analysis is crucial for maintaining smooth business operations and ensuring that organizations can adapt to changing conditions.

IS/IT service mapping is carried out to determine what services are provided by an information system in serving both internal institutions and external users. At the Daniel S. Law Library, system-based services such as repositories, Digilev, and *the* Danlev *Catalog* are an important foundation for the smooth operation of the library and support research needs that are highly dependent on the availability and stability of access.

Table 4. IS/IT Service Mapping

No	Information System	Impact if IS is down
1	Digilev	Hinders access to active research, especially for students who are writing their thesis/dissertation and faculty members who are abroad
2	Institutional Repository	Declining academic reputation and accreditation, inability to access scientific publications, and potential loss of important documents such as theses/dissertations.

3	Danlev *Catalog* (based on SLiMS)	Unable to search for information and collections in the library
4	Court ruling	Disruption to access to legal documents but no impact on the library's main services.
5	Internal Archiving System	Services may be disrupted but are rarely used and can only be accessed locally (LAN)

Based on interviews conducted to determine the criticality level of information systems at the Daniel S. Law Library, a classification of the impact level of disruptions to library services and operational continuity was obtained. To strengthen this assessment framework, reference was made to FIPS 199 (Federal Information Processing Standards Publication 199), which establishes three levels of potential impact on an organization in the event of an information system security breach, specifically in terms of *confidentiality*, integrity, and *availability* (Technology, 2004) .

1. High
   The information system has a significant impact and side effects on the institution and the continuity of an organization, as well as on external parties or users associated with the academic community and researchers.
2. Moder*ate*
   Information systems influence the main activities of each work unit in an institution and have a serious impact on libraries, as well as affecting relationships with external parties within a limited scope.
3. Low
   Information systems only impact institutional support activities or are only used internally on a small scale in libraries.
   The results of the analysis of the business impact categories on the Daniel S. Lev Law Library information system are presented in Table 5.

Table 5. Disruption Impact Categories Based on FIPS 199

No	**Information System**	**Impact Category**	**Description**
1	Digilev	High	Frequently accessed for research purposes, including by foreign academics. Very important for academic continuity.
2	Institutional Repository	High	Directly related to accreditation and national regulations. Must be available *online,* especially during thesis and scientific publication periods.
3	Danlev *Catalog* (based on SLiMS)	Moderate	Used to search for information and collections in the library. However, a manual master book is available in Excel as *a backup* search when the system is *down.*

4	Court Decision	Moderate	Used for internal jurisprudence access. Does not have a significant impact on the library's main services
5	Internal Archiving System	Low	Access is local (LAN) and can only be accessed by internal staff with low frequency of use.

Determining *the Recovery Point Objective* (RPO) and *Recovery Time Objective* (RTO) for each IS/IT service is the next step in analyzing business impact. *Recovery Time Objective* (RTO) is the maximum acceptable time for a system to be restored to normal operation after a disruption, while *Recovery Point Objective* (RPO) is the amount of data loss that is still acceptable in the event of system damage or disruption. For the Daniel S. Lev Law Library, this is presented in Table 6.

Table 6. Identification of *Recovery Time Objective* (RTO) and *Recovery Point Objective* (RPO)

No	Information System	RTO	RPO	Impact Level	Description
1	Digilev	24-72 hours	< 1 month	High	Experienced *downtime* for up to a month, but it was still manageable because there was a manual ledger in Excel and monthly backups to staff laptops.
2	Institutional Repository	< 24 hours	<1 week	High	Critical system for accreditation. Hosted in *the cloud* and must always be available. Risk of damage can be minimized with *a firewall* and GCP.
3	Danlev *Catalog* (based on SLiMS)	< 3 days	< 1 month	Moderate	If *downtime* occurs, searches can still be performed manually via Excel. Catalog *backups* are prepared offline.
4	Court Decision	< 1 week	< 1 month	Moderate	The system is used internally only and does not have high urgency in recovery.
5	Internal Filing System	< 1 week	< 1 month	Low	The system is LAN-based, only used in the

					office, and access frequency is quite low. *Backups* are performed manually and rarely changed.

The final stage in this analysis process is to determine the IS/IT that is a priority at the Daniel S. Law Library. IS/IT priorities are determined by processing the results of the analysis of the impact of risk on the institution's business and determining the *Recovery Time Objective* (RTO) and *Recovery Point Objective* (RPO) values for each IS/IT.

Table 7. Information System Recovery Priorities

No	Priority	Information System	Priority Order
1	High	Institutional Repository	1
2	High	Digilev	2
3	Medium	Danlev *Catalog* (based on SLiMS)	3
4	In progress	Court Decision	4
5	Low	Internal Filing System	5

Recovery Strategy

A Recovery Strategy is a set of steps taken to restore a system to its normal state after a disruption or failure (Wu & Wang, 2021) . In practice, the recovery process requires various preparations, such as the availability of hardware and software that can be used to restore services.

To design an effective recovery strategy, it is important to consider the extent of damage caused by the disruption or disaster. Threats to information systems and information technology (IS/IT) are usually described through analyzed risk attributes, so a recovery strategy based on these results is required. As an illustration, the following is an example of an information system recovery process table at the Daniel S. Law Library.

Table 8. *Recovery Strategy*

No	Threat	Constraints	Recovery Process
1	Server *Down*	Server cannot be accessed due to physical or logical damage	Replace with a backup server and ensure that the latest data backup can be restored
2	Power Outage	Power loss, unstable voltage	Provide UPS and generator to maintain power stability and prevent equipment damage
3	Virus attacks	Corrupted files, slow system, data loss	Performing regular antivirus *scans*, installing security *patches*, and *backing up* and *restoring* the system

4	*Cyber Threat*	Hacking due to weak *passwords* or system vulnerabilities	Strengthen authentication (strong *passwords*, MFA), regularly *update* the system, and conduct regular security audits
5	*Human Error*	Data loss due to input errors, accidental deletion	Implement *auto-save* systems, activity *logging*, and employee training
6	*System Failure*	System crashes, *software* malfunctions	Prepare backup *images*, use *redundant software*, and *monitor* system performance
7	*Human Deliberate*	Asset theft or data leakage	Install CCTV, restrict access to server rooms, and audit system *logs*
8	Lightning	Damage to servers, LAN networks, electronic devices	Electrical *grounding*, install *lightning arresters,* and use surge protectors
9	Earthquake	Building damage, physical collections, and servers	Store data in the cloud or *off-site* backup, and have an evacuation plan and physical disaster SOP
10	Fire	Collections burned, services paralyzed	Use *fire extinguishers*, *smoke detectors,* and external digital backups

Documentation

Documentation is the final stage, which aims to document all the results of *the Disaster Recovery Plan* design in the form of a structured document that is ready to be used in the event of a disruption to the information system. The preparation of this document refers to the NIST SP 800-34 Rev. 1 standard, with the content and procedures adjusted to the needs and characteristics of the Daniel S. Lev Law Library. The main function of this documentation is to serve as an institutional guideline in ensuring the continuity of information services when incidents occur, both technical and major disasters. The complete results of this *disaster recovery plan* document are submitted to the Daniel S. Lev Law Library as a form of contribution and proposal in supporting efforts to improve the readiness and recovery of the library's information system in the event of a disaster or threat.

4. CONCLUSION

This study has designed a DRP document based on the NIST SP 800-34 Rev. 1 approach, which includes asset and risk identification, impact level classification using FIPS 199, and determination of RTO and RPO for each information system. The analysis results show that the Digilev and Repository s have the highest system urgency levels and need to be the top priority in the recovery strategy. Meanwhile, other systems such as *the* Danlev *Catalog*, Court Decisions, and Local Archiving System are assessed as having moderate to low impact, but still require special handling in emergency recovery planning. As a follow-up measure, it is recommended that the Daniel S. Lev Law Library:

a. Conduct *drills* on system disruption scenarios and periodically validate DRP documents.
b. Conduct internal staff training on data recovery and information system management during crises.
c. Provide basic infrastructure such as UPS, security monitoring systems, and implement more comprehensive data security policies.

d. Use this DRP document design as a reference for creating institutional policies that are distributed in a limited but strategic manner to all relevant units.

Through the preparation of this NIST SP 800-34-based DRP, the research not only provides practical solutions for the Daniel S. Lev Law Library, but also contributes scientifically as a model for implementing disaster recovery planning for law libraries or similar information institutions in Indonesia. With the design of this DRP document, it is hoped that the Daniel S. Lev Law Library can improve institutional resilience to system disruptions and ensure continuity of information services amid various risks that may occur.

REFERENCES

Afifah, N., Khotimah, K., Pujiastuti, B., Nofitasari, D., Arfanandha, A. M., & Fauzi, M. R. (2019). Rancangan Dokumen Disaster Recovery Plan pada Perpustakaan Daerah Purbalingga. Dalam *CITISEE 2019 - Conference on Information Technology, Information System and Electrical Engineering* (hlm. 105–110). Purwokerto: Universitas Amikom. https://citisee.amikompurwokerto.ac.id/content/proceedings/2019

Balaji, S., Shreshta, L., & Sujatha, K. (2024). A Study on Risk Management in Corporate Business. *Involvement International Journal of Business*, *1*(3), 197-209. DOI 10.62569/iijb.v1i3.26

Beretas, C. (2024). Information systems security, detection and recovery from cyber attacks. *Universal Library of Engineering Technology*, *1*(1). DOI 10.70315/uloap.ulete.2024.0101005

Computer Security Division IT Laboratory NIST. (2004). *FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems*. U.S: NIST. DOI 10.6028/NIST.FIPS.199

Dada, K. S. J., Hamza, J. M., & Mohammed, H. A. (2025). Disaster Risk Management in Libraries and Information Centers: Global Strategies, Challenges, Policy and Recommendations. *International Journal of Disaster Risk Management*, *7*(1), 203-214. DOI 10.18485/ijdrm.2025.7.1.11

Dekker, M. M., Van Lieshout, R. N., Ball, R. C., Bouman, P. C., Dekker, S. C., Dijkstra, H. A., ... & van den Akker, M. (2022). A next step in disruption management: combining operations research and complexity science. *Public Transport*, *14*(1), 5-26. DOI 0.1007/s12469-021-00261-5

Di Sutam, E., Pei, F. L., Jia, J. T., Muhammad, N. A., Ab-Samat, H., Jeng, F. C., ... & Sirivongpaisal, N. (2024). A comparative study on user satisfaction from manual to online information system using define-measure-analyze-improve-control (dmaic) in service administrative process. *Journal of Advanced Research Design*, *122*(1), 27-45. DOI 10.37934/ard.122.1.2745

Enakrire, R. T., Oladokun, B. D., Nsirim, O., & Gaitanou, P. (2024). Paperless libraries: The trending way to go in the fifth industrial revolution. *Business Information Review*, *41*(4), 164-173. DOI 10.1177/02663821241289793

Garnett, J. (2021). Academic libraries–Changing the approach: Resilience building against disruptive events and the contribution to disaster risk reduction frameworks. *New Review of Academic Librarianship*, *27*(1), 113-129. DOI 10.1080/13614533.2019.1703767

Ikenwe, I. J., & Udem, O. K. (2022). Innovative digital transformation for dynamic information service sustainability in university libraries in Nigeria. DOI 10.12775/FT.2022.004

International Standard Organization ISO/IEC 27001. (2022). *Information Security, Cybersecurity and Privacy Protection Information Security Management Systems Requirements*. Geneva: International Standard Organization.

Magsi, I., Shaheen, N., Channar, W. A., Ali, M., Lakho, Z., & Ahmed, A. (2025). Cyber-Security Challenges in Digital Libraries. *Review Journal of Social Psychology & Social Works*, *3*(1), 344-350. DOI 10.71145/rjsp.v3i1.102

NIST Special Publication 800-34 Rev 1. (2010). *Contingency Planning Guide for Information Systems*. Washington: NIST. DOI 10.6028/NIST.SP.800-34r1

Onunka, O., Onunka, T., Fawole, A. A., Adeleke, I. J., & Daraojimba, C. (2023). Library and information services in the digital age: Opportunities and challenges. *Acta Informatica Malaysia*, *7*(1), 113-121. DOI 10.26480/aim.02.2023.113.121

Oyedokun, T. T. (2025). Navigating the dynamics of present-day academic libraries: An in-depth analysis of strategies, challenges, and emerging trends. *IFLA Journal*, *51*(2), 470-489. DOI 10.1177/03400352241291907

Rahmani, M. (2025). Strategic risk management in public library services: Approaches to prioritization and mitigation. *Malaysian Journal of Library and Information Science*, *30*(1), 78-111. DOI 10.22452/mjlis.vol30no1

Revathi, N., & Mohan, V. V. (2022). Paradigm shift of library and information services with special reference to mobile information services in 21st century. *International Journal of Research in Library Science (IJRLS)*, *8*(1), 15-25. DOI 10.26761/IJRLS.8.1.2022.1492

Sugiyono. (2022). Metode Penelitian Kualitatif. Bandung: Alfabeta.

Taherdoost, H. (2023). An overview of trends in information systems: Emerging technologies that transform the information technology industry. *Taherdoost, H.(2023). An overview of trends in information systems: emerging technologies that transform the information technology industry. Cloud Computing and Data Science*, 1-16. DOI 10.37256/ccds.4120231653

Wu, J., & Wang, P. (2021). Post-disruption performance recovery to enhance resilience of interconnected network systems. *Sustainable and Resilient Infrastructure*, *6*(1-2), 107-123. DOI 10.1080/23789689.2019.1710073