Equivalent: Jurnal Ilmiah Sosial Teknik
Volume 8, Issue 3, 769-786
e_ISSN: 2775-0833
https://jurnalequivalent.id/index.php/jequi/index
DOI: doi.org/10.59261/jequi.v8i3.340

NIST SP 800-34-Based Disaster Recovery Plan Framework for the National Committee for Sharia Economics

Khalil Mojadidi* Universitas Bina Nusantara, Indonesia
Abba Suganda Girsang Universitas Bina Nusantara, Indonesia

***Corresponding author:**
Khalil Mojadidi, Universitas Bina Nusantara, Indonesia ✉khalil.moja@pu.go.id

Article Info:
Article history:
Received: May 12, 2026
Revised: June 25, 2026
Accepted: July 04, 2026

Keywords:
Disaster Recovery Plan; Business Continuity; Risk Assessment
NIST SP 800-34.

Abstract

Background: In today's digital era, information technology (IT) infrastructure is critical to organizational operations, making Disaster Recovery Planning (DRP) essential for business continuity. Institutions managing strategic data assets, such as KNEKS, must address risks from disasters, cyberattacks, and infrastructure failures during PDES development.
Objective: This study aims to identify KNEKS's disaster recovery requirements under current and future PDES conditions and to develop a comprehensive DRP framework based on NIST SP 800-34.
Methods: A qualitative case study approach was employed using NIST SP 800-34 Rev. 1 as the primary framework, complemented by FIPS 199, SNI ISO 31000, and NIST SP 800-53. Data were collected through semi-structured interviews with IT managers and system administrators, supported by document analysis. Triangulation and member checking were used to ensure validity.
Results: The assessment revealed significant gaps in disaster recovery readiness, particularly in formalized policies, technical redundancy, and impact analysis procedures. Based on these findings, a tailored DRP framework was developed, incorporating activation, recovery, and reconstitution phases while maintaining scalability for future PDES expansion.
Conclusion: A comprehensive NIST SP 800-34-based DRP is essential to ensure KNEKS's operational continuity. The proposed framework offers a structured and scalable approach to disaster recovery and provides a practical model for emerging public-sector, data-intensive institutions.

To cite this article: Mojadidi, K., & Girsang, A. S. (2026). NIST SP 800-34-Based Disaster Recovery Plan Framework for the National Committee for Sharia Economics. *Equivalent: Jurnal Ilmiah Sosial Teknik*, 8(3), 769-786. https://doi.org/10.59261/jequi.v8i3.340

INTRODUCTION

In the contemporary business landscape, information technology (IT) has become the backbone of global operations. Consequently, the importance of robust and effective Disaster Recovery Planning (DRP) cannot be overstated (Kesa, 2023). Organizations of all scales are susceptible to disasters, as evidenced by several significant IT-related incidents in recent history, as shown in Table 1. These incidents underscore the critical need for comprehensive disaster recovery strategies across all organizations, regardless of their size or industry.

The National Committee for Sharia Economics and Finance (Komite Nasional Ekonomi dan Keuangan Syariah, or KNEKS), the subject of this case study, recognizes this imperative and seeks to develop its own DRP. KNEKS aims to enhance the development of the sharia economic and financial ecosystem to support national economic growth. Its vision is to become a leading institution in sharia economic data and analysis by establishing its own Sharia Economic Data Center (*Pusat Data Ekonomi Syariah*, or PDES).

To realize this vision and ensure the resilience of its operations, KNEKS must address several key challenges: mitigating potential losses due to human actions or natural disasters, ensuring the continuity of critical business processes in the face of disruptions, and maintaining system availability to support seamless business services (Suresh et al., 2020). While effective control and management can reduce these risks, they cannot be eliminated entirely. This reality highlights the necessity of comprehensive contingency planning.

Table 1. IT incidents declared around the World

Year of Declaration	Country Affected	Description
2007	Australia	Australia's healthcare payroll system failure by IBM, affecting 80,000 healthcare professionals.
2013	USA	US healthcare facility system failure, disrupting critical services.
2017	Global	WannaCry ransomware cyber-attacks crippling operations across multiple sectors.
2023	Indonesia	BSI cyber-attack, compromising 1.5 TB of sensitive data.
2020	USA	SolarWinds supply chain attack compromising 18,000+ organizations including government agencies.
2021	USA	Colonial Pipeline ransomware attack causing fuel supply disruption across the Eastern United States.
2022	Costa Rica	Conti ransomware attack on government systems, forcing a national emergency declaration.
2024	Indonesia	Pusat Data Nasional Sementara (PDNS) ransomware attack disrupting 282 government institution services.

Disaster Recovery Planning (DRP) is a strategic process that aims to ensure the continuity of critical business functions in the face of disruptive events (Sawalha, 2021; Stamenkov, 2025). Al Hassan defines DRP as a process that identifies, assesses, and mitigates risks associated with IT use in businesses (Al Hassan, 2017; Almutawa, 2026). DRP is an ongoing process involving continuous planning, development, testing, and implementation of disaster recovery procedures (Mohamed, 2014; Craven & Tomlinson, 2026). DRP is positioned as a crucial component of Business Continuity Planning (BCP), with a specific focus on recovering IT infrastructure and systems (Craven & Tomlinson, 2026; Swanson et al., 2010). This highlights the integral role of IT in modern business operations and the need for targeted recovery strategies for technology-dependent functions.

Key aspects of DRP include the identification of potential threats and vulnerabilities, determination of critical resources required for business continuity during disasters, and establishment of mechanisms to restore business operations to normalcy (Tatineni, 2023) (Stamenkov, 2025). Successful implementation of DRP requires strong management support and commitment, adequate resource allocation, and alignment with organizational goals and objectives (Ashrafi & AlKindi, 2022). A dedicated DRP team is trained in risk analysis and the coordination of recovery efforts (Ashrafi & AlKindi, 2022; Snedaker, 2013). Regular documentation and testing are also required to ensure effectiveness and reliability (Ashrafi & AlKindi, 2022). Business Impact Analysis (BIA) and risk analysis are critical components of DRP, helping organizations prioritize applications and services for recovery (Arroyo-Melendez, 2026; Saleem, 2008). These processes ensure that recovery efforts are focused on the most critical business functions, thereby optimizing resource allocation during disaster response.

To achieve these objectives, this study will utilize established DRP frameworks, primarily NIST SP 800-34, complemented by other compatible standards such as NIST SP 800-53, NIST FIPS 199, and ISO 31000. This approach provides comprehensive guidelines for developing a robust DRP tailored to KNEKS's unique needs and circumstances. Beyond its practical contributions, this study advances DRP theory by demonstrating how maturity-based gap analysis can inform phased DRP implementation strategies for emerging institutions. The findings provide empirical evidence for the adaptability of NIST SP 800-34 in non-traditional public sector contexts, offering a replicable model for similar organizations in developing countries undergoing digital

transformation initiatives (Ahmad et al., 2021; Hendaryatna et al., 2023).

NIST SP 800-34 was chosen as the primary framework mainly for its relevance to the public sector. As a product of a U.S. government agency, NIST SP 800-34 demonstrates a deep understanding of the unique needs and challenges faced by public sector organizations like KNEKS (Lubis et al., 2026). The framework provides thorough guidance from the planning stage through implementation and maintenance of the DRP. It covers all crucial aspects of DRP development, including risk assessment, business impact analysis, recovery strategies, recovery procedures, testing, and plan maintenance (Epstein & Khan, 2014; Ferrer & Mandigma, 2026). NIST SP 800-34 also offers comprehensive guidelines for risk assessment and business impact analysis (Hendaryatna et al., 2023). This is particularly crucial for KNEKS, given the complexity and sensitivity of sharia economic data managed by PDES.

Several previous studies have applied NIST SP 800-34 in various organizational contexts. Dwi et al. (2023) analyzed DRP implementation at PT Wijaya Karya using the NIST SP 800-34 framework in a state-owned construction enterprise. Alifian and Priharsari (2021) developed a DRP for a national IT company using the same framework. Supriyanto et al. (2019) applied NIST SP 800-34 to the IT department of PT Pupuk Kalimantan Timur (Dearniwati et al., 2025). However, these studies predominantly focused on private-sector or industrial organizations with established IT infrastructure. The application of NIST SP 800-34 to public sector institutions managing specialized macroeconomic data, particularly those in the early stages of data center development, remains underexplored in the literature.

The research gap addressed by this study lies in the absence of DRP frameworks specifically tailored for emerging public sector financial institutions that manage sensitive sharia economic data. While existing literature extensively covers DRP implementation in mature organizations with established IT ecosystems, there is a notable lack of studies examining how frameworks like NIST SP 800-34 should be adapted for institutions that are simultaneously building their data center infrastructure and developing their DRP capabilities. KNEKS presents a unique case, as it is in the process of establishing the Sharia Economic Data Center (PDES), requiring a DRP that is both immediately functional and scalable to accommodate future growth. This dual requirement distinguishes the current study from prior research that typically addresses organizations with static IT environments.

The novelty of this research lies in three aspects: first, the integration of multiple complementary frameworks (NIST SP 800-34, FIPS 199, ISO 31000, and NIST SP 800-53) to create a holistic DRP design rather than relying on a single standard; second, the development of a phased implementation roadmap that accounts for the transitional nature of KNEKS from a committee-level organization to a data-intensive institution; and third, the contextualization of international DRP standards within the Indonesian public sector regulatory environment, bridging the gap between global best practices and local governance requirements (Cedergren et al., 2026; Hassel & Cedergren, 2021). Therefore, this study contributes to disaster recovery planning literature by proposing a maturity-gap-driven DRP framework tailored to emerging public sector institutions undergoing digital transformation.

This study aims to identify the disaster recovery requirements of the National Committee for Sharia Economics (KNEKS) under its current operational environment and the future Sharia Economic Data Center (PDES) scenario. Furthermore, it aims to assess the organization's disaster recovery readiness and develop a Disaster Recovery Plan (DRP) framework based on NIST SP 800-34 to support business continuity and information system resilience. This study contributes to the literature in three ways. First, it extends the application of NIST SP 800-34 to emerging public sector institutions managing specialized economic data. Second, it proposes a maturity-gap-based implementation approach for prioritizing DRP development activities. Third, it demonstrates how international disaster recovery standards can be adapted to the Indonesian public sector governance context.

METHOD

This research adopted an explorative and qualitative approach to understand and design a DRP tailored to KNEKS. The study employed a case study method, which is particularly well-suited for examining complex phenomena within their real-life context. This approach allowed

for:

An in-depth exploration of KNEKS as a specific organization.

A holistic view of the organization's current DRP practices, challenges, and needs.

The ability to consider multiple variables and their interactions within the organizational context.

The research was conducted over a six-month period from January to June 2026. The study followed a systematic five-phase process: (1) preliminary assessment of KNEKS's current IT infrastructure and organizational structure through document review; (2) semi-structured interviews with five key informants comprising the Head of IT Division, two system administrators, one business continuity coordinator, and one senior management representative; (3) analysis of existing organizational documents including IT policies, network topology diagrams, and current backup procedures; (4) maturity assessment of DRP components using a 1-to-5 scale derived from interview responses and document analysis; and (5) framework design and validation through iterative consultation with KNEKS stakeholders.

To ensure the credibility and trustworthiness of the findings, this study employed multiple data validation techniques. Triangulation was achieved by cross-referencing data from three sources: interview transcripts, organizational documents, and direct observations of IT infrastructure. Member checking was conducted by presenting preliminary findings to key informants for verification and feedback, ensuring that the interpretations accurately reflected organizational realities. Additionally, an audit trail was maintained throughout the research process, documenting all data collection activities, analytical decisions, and framework development iterations to ensure methodological transparency and reproducibility (Creswell & Creswell, 2018; Rambharose, 2026).

To ensure a comprehensive and nuanced understanding of the case study object, this research employed multiple qualitative data collection methods:

Semi-structured interviews:

1) Participants included key stakeholders such as IT managers, system administrators, and business continuity planners.
2) The purpose was to gain insights into current DRP practices, perceived risks, and recovery needs.
3) The approach used open-ended questions to allow for detailed responses and follow-up inquiries.

Document analysis:

1) Materials included existing organizational documents such as current DRP plans (if any), IT policies, business continuity plans, and incident reports.
2) The purpose was to identify gaps in current practices and areas for improvement.
3) The approach involved systematic review and content analysis of relevant documents.

The research process followed a structured approach based on the guidelines outlined in NIST SP 800-34 for information system contingency planning. The stages were as follows:

1) Developing a Disaster Recovery Policy.
2) Conducting Business Impact Analysis.
3) Identifying Preventive Controls.
4) Developing Disaster Recovery Strategies.
5) Creating Recovery Plans.
6) Planning for Testing, Training, and Drills.
7) Creating a Maintenance Plan.

RESULTS AND DISCUSSION

Result

Following the analysis of data gathered through semi-structured interviews and direct observations, a Disaster Recovery Plan (DRP) framework was designed to address the specific requirements of KNEKS. Table 2 provides a summary of the DRP component evaluations proposed for the organization, illustrating the assessment of current readiness across identified areas. This

evaluation uses a maturity scale from 1 to 5, where a value of 1 indicates that KNEKS has no established concept for the component, and a value of 5 signifies that the relevant process is fully established and functioning effectively within the institution's operations. Each component is also categorized based on its implementation priority, namely short-term or long-term. This categorization helps KNEKS plan DRP implementation gradually and focus on the most critical components in the short term. Table 3 presents the gap analysis between current readiness levels and target maturity scores for each DRP component.

The readiness scores presented in Table 2 were derived from a structured assessment process involving semi-structured interviews with five key informants at KNEKS. Each DRP component was evaluated using a maturity scale from 1 to 5, where 1 indicates no established concept and 5 indicates a fully established and functioning process. For components assessed by multiple informants or containing multiple sub-variables, decimal values represent the arithmetic mean of individual assessments. For example, a score of 2.33 for the Recovery Phase component reflects the average across three sub-variable assessments rated 2, 2, and 3, respectively. The implementation priority (short-term or long-term) was determined based on the criticality of each component for immediate operational continuity and the feasibility of implementation given current organizational resources.

Table 2. Summary of the DRP component evaluations proposed for the organization

Stages	Components	Readiness	Implementation Plan
Developing Disaster Recovery Policy	Objectives	2	Short-term
	Scope	2	Short-term
	Assumptions	1	Short-term
	Exceptions	4	Short-term
	Roles and Responsibilities	3	Short-term
	Coordination with Related Plans	1	Long-term
	Communication	-	-
Conducting Business Impact Analysis	Context Establishment	2	Short-term
	Risk Assessment	2	Short-term
	Risk Treatment	2	Short-term
	Monitoring and Evaluation	1	Short-term
	Recording and Reporting	1	Short-term
	Communication and Consultation	1	Short-term
	Affected Entities	2	Short-term
	Security Information and Event Management	1.6	
	Identifying process/system criticality (MTD, RTO, RPO)	2	Short-term
	Identifying Recovery Priorities	4	Short-term
Identifying Preventive Controls	Control Categorization	-	-
Developing Disaster Recovery Strategies	Backup and recovery (basic)	4	Short-term
	Backup and recovery (advanced)	1.33	
	System and network redundancy	1	Short-term
	Alternative storage site (basic)	4	Short-term
	Alternative storage site	1	

Stages	Components	Readiness	Implementation Plan
	(advanced)		
Creating Recovery Plans	Activation Phase	1	Short-term
	Recovery Phase	2.33	Short-term
	Reconstitution Phase	1	Short-term
	Communication and Coordination	4	Short-term
	Public Relations Communication Management	-	-
Planning for Testing, Training, and Drills	Tests Plan	1	Short-term
	Training Plan	3	Short-term
Creating a Maintenance Plan	Periodic review	3	Short-term
	Periodic Updates	3	Short-term
	Lesson Learned	3	Short-term

Source: Research Data

Table 3. Gap Analysis

Stages	Components	Readiness	Target	Gap
Developing Disaster Recovery Policy	Objectives	2	3	-1
	Scope	2	3	-1
	Assumptions	1	3	-2
	Exceptions	4	3	1
	Roles and Responsibilities	3	3	0
	Coordination with Related Plans	1	3	-2
	Communication	-		
Conducting Business Impact Analysis	Context Establishment	2	3	-1
	Risk Assessment	2	3	-1
	Risk Treatment	2	3	-1
	Monitoring and Evaluation	1	3	-2
	Recording and Reporting	1	3	-2
	Communication and Consultation	1	3	-2
	Affected Entities	2	3	-1
	Security Information and Event Management	1.6	3	-1,4
	Identifying process/system criticality (MTD, RTO, RPO)	2	3	-1
	Identifying Recovery Priorities	4	3	1
Identifying Preventive Controls	Control Categorization	-		
Developing Disaster Recovery Strategies	Backup and recovery (basic)	4	3	1
	Backup and recovery (advanced)	1.33	3	-1,66
	System and network redundancy	1	3	-2
	Alternative storage site (basic)	4	3	1
	Alternative storage site (advanced)	1	3	-2

Stages	Components	Readiness	Target	Gap
Creating Recovery Plans	Activation Phase	1	3	-2
	Recovery Phase	2.33	3	-0,66
	Reconstitution Phase	1	3	-2
	Communication and Coordination	4	3	1
	Public Relations Communication Management	-		
Planning for Testing, Training, and Drills	Tests Plan	1	3	-2
	Training Plan	3	3	0
Creating a Maintenance Plan	Periodic review	3	3	0
	Periodic Updates	3	3	0
	Lesson Learned	3	3	0

Source: Research Data

The gap analysis reveals that the most critical deficiencies (gap value of -2) are concentrated in five components: Assumptions; Coordination with Related Plans; Monitoring and Evaluation; Recording and Reporting; Communication and Consultation; System and Network Redundancy; Activation Phase; Reconstitution Phase; and Test Plan. These components represent the highest-priority areas requiring immediate attention in KNEKS's short-term DRP implementation strategy. The negative gaps indicate that KNEKS has not yet developed formalized processes for these critical areas, posing significant risks to operational continuity in the event of a disaster. The structure of the list has been standardized for clarity and consistency, and "Tests Plan" has been corrected to "Test Plan" in accordance with common disaster recovery terminology.

Conversely, four components show positive gaps (value of +1): Exceptions; Identifying Recovery Priorities; Backup and Recovery (basic); Alternative Storage Site (basic); and Communication and Coordination. These components exceed the target maturity level, indicating that KNEKS has established foundational capabilities in certain operational areas, largely influenced by existing Ministry of Finance standards and procedures. The overall pattern suggests that while KNEKS possesses basic operational resilience capabilities, the organization still lacks fully formalized and documented procedures necessary for a comprehensive disaster recovery program aligned with established disaster recovery planning frameworks.

Discussion

The results of the readiness assessment and gap analysis reveal a clear distinction between KNEKS's current operational capabilities and the requirements of a comprehensive Disaster Recovery Plan (DRP). While basic recovery mechanisms and certain administrative roles are already influenced by existing Ministry of Finance standards, significant gaps remain in formalized policies, advanced technical redundancies, and standardized impact analysis. This discussion evaluates how these findings inform the proposed DRP framework, prioritizing short-term interventions for critical infrastructure while aligning long-term strategies with KNEKS's evolving digital ecosystem.

The findings of this study are broadly consistent with previous research that applied the NIST SP 800-34 framework in organizational disaster recovery planning. For example, Dwi Pamungkas et al. (2023) reported that organizations with established IT governance structures generally demonstrate stronger readiness in backup management and recovery prioritization than in formal disaster recovery documentation and testing procedures. Similar patterns were observed in KNEKS, where the readiness scores for basic backup and recovery (4.0) and recovery prioritization (4.0) exceeded the target maturity level, while activation procedures, recovery reconstitution planning, and testing programs remained underdeveloped. This finding suggests that operational recovery activities tend to evolve earlier than formalized governance mechanisms in many organizations implementing DRP initiatives.

The results also support the findings of Alifian and Priharsari (2021), who emphasized

that the successful implementation of NIST SP 800-34 requires not only technical recovery capabilities but also documented policies, clearly defined responsibilities, and continuous testing mechanisms (Dwi et al., 2023). In the present study, several governance-related components including assumptions, coordination with related plans, monitoring and evaluation, and testing plans recorded the largest maturity gaps. These findings reinforce the argument that disaster recovery readiness should be viewed as an organizational capability rather than merely a technical infrastructure issue.

However, this study differs from previous research in several important aspects. Earlier studies conducted at PT Wijaya Karya (Dwi et al., 2023) and PT Pupuk Kalimantan Timur (Supriyanto et al., 2019) focused on organizations with relatively mature IT infrastructures and operational environments (Dwi et al., 2023). In contrast, KNEKS is currently undergoing a digital transformation process while simultaneously preparing the establishment of the Sharia Economic Data Center (PDES). As a result, disaster recovery planning must address not only existing operational risks but also future infrastructure expansion. This transitional condition creates additional complexity that is not widely discussed in previous NIST SP 800-34 implementation studies.

Another notable finding concerns the concentration of maturity gaps within activation, recovery reconstitution, and testing components. From a theoretical perspective, this indicates that organizations in the early stages of data center development tend to prioritize preventive and operational controls before investing in comprehensive recovery governance mechanisms. This pattern extends existing DRP literature by suggesting that disaster recovery maturity develops progressively across different capability domains rather than uniformly across all framework components. Therefore, the phased implementation strategy proposed in this study provides empirical support for a maturity-driven approach to DRP development in emerging public-sector institutions.

The findings of this study carry implications beyond the Indonesian context. The phased DRP implementation approach developed for KNEKS offers a transferable model for public sector institutions in other developing countries that are in the early stages of digital transformation and data center development. The integration of international standards (NIST SP 800-34) with local regulatory frameworks (Indonesian ISO 31000 adaptation) demonstrates how global best practices can be contextualized for national governance environments. This is particularly relevant for institutions in Organization of Islamic Cooperation (OIC) member countries that are establishing similar sharia economic data management capabilities, as they face comparable challenges in balancing international IT governance standards with local institutional capacities (Singh & Alshammari, 2023; Singh et al., 2021).

From a cross-cultural perspective, this study reveals that DRP frameworks originally designed for Western government agencies require significant adaptation when applied to institutions in developing countries. The maturity assessment revealed that organizational culture, resource constraints, and regulatory differences substantially influence DRP readiness. For instance, the reliance on Ministry of Finance standards in lieu of dedicated DRP policies reflects a hierarchical governance structure that shapes how disaster recovery responsibilities are distributed and managed, a factor not adequately addressed in the original NIST framework.

This study acknowledges several limitations. First, the research is based on a single case study of KNEKS, which limits the generalizability of findings to other organizations with different structural and operational characteristics. Second, the maturity assessment relies on self-reported data from five key informants, which may introduce subjectivity despite the use of triangulation and member checking. Third, the proposed DRP framework has not yet undergone actual disaster scenario testing, meaning its effectiveness remains theoretical. Fourth, the study was conducted during KNEKS's transitional phase toward establishing PDES, and the organizational landscape may have evolved since data collection. Future research should consider longitudinal studies tracking DRP implementation outcomes and comparative case studies across multiple public sector institutions to validate and refine the proposed framework.

Disaster Recovery Policy Development

foundation of an effective disaster recovery plan (DRP) lies in clear and well-defined policies. For KNEKS, these policies must align with relevant laws, directives, standards, and guidelines while also addressing the organization's specific operational needs.

KNEKS needs to establish a structured disaster recovery team, initially involving:

1) Creation of a centralized council representing various departments.
2) Appointment of a team leader to oversee recovery efforts.
3) Designation of coordinators and specialized recovery teams.

Key roles within the disaster recovery team include:

1) Team Leader: Oversees the recovery of all systems and business functions.
2) Recovery Coordinator: Directs disaster response and recovery processes.
3) Disaster Assessment Team: Assesses disaster impact and determines recovery priorities.
4) Communication Team: Manages internal and external communications.
5) Network Recovery Team: Restores network infrastructure and connectivity.
6) Server Recovery Team: Restores server infrastructure and related services.
7) Backup & Restore Team: Conducts regular data backups and performs data restoration after a disaster.
8) Application Recovery Team: Restores critical business applications.

In addition to roles and responsibilities, the DRP policy should address:

1) Scope: Specifies the conditions under which the DRP is activated.
2) Resource Requirements: Details personnel, technological, and infrastructure needs for recovery.
3) Assumptions: Defines underlying conditions or dependencies required for effective DRP implementation.
4) Exclusions: Identifies recovery activities that are not included within the plan.

As KNEKS develops its infrastructure, including the establishment of a data center by the third year, it will also need to consider setting up a disaster recovery center (DRC) in a separate location, allocating additional personnel for disaster recovery operations, and regularly updating the DRP to reflect ongoing infrastructural and operational changes.

Risk Assessment and Business Impact Analysis

KNEKS should adopt a structured approach to risk assessment based on risk management guidelines for the Indonesian public sector (heavily based on ISO 31000). The process includes:

1) Setting the risk context aligned with strategic goals.
2) Listing and analyzing risks.
3) Evaluating and prioritizing risks for mitigation.
4) Regular documentation and monitoring.

Before evaluating risks, KNEKS needs to:

1) Specify the risk appetite to align with organizational goals.
2) Identify, list, and categorize stakeholders.
3) Establish risk assessment criteria, including likelihood and impact criteria.

Table 4, 5, and 6 provide examples of detailed criteria for likelihood and impact. Using likelihood and impact values from risk analysis as inputs, the overall risk level can be determined using a risk analysis matrix as presented in Table 7. In the context of disaster recovery planning, where recovery takes precedence over prevention, high-impact but rare risks require greater attention than frequent but low-impact ones.

Equations should be written using native MS Word Equation Editor or MathType. Image-based equations should be avoided because they reduce quality during PDF production. Each equation should be numbered consecutively, with the number placed on the right side. Additionally, all variables or parameters should be clearly explained upon first use, particularly immediately following the equation. The sample equation is in table 4.

Table 1. Likelihood criteria example

Likelihood Level	Value	Likelihood Criteria	
		Percentage	Frequency (per year)
Rare	1	x =< 5%	x =< 2 times
Unlikely	2	5% < x =< 10%	2 < x =< 5 times
Moderate	3	10% < x =<20%	6 < x =< 9 times
Likely	4	20% < x =<50%	10 < x =< 12 times
Almost certain	5	x > 50%	x > 12 times

Source: Research Data

Table 2. Financial impact criteria example

Impact	Value	Explanation
Insignificant	1	x =< 0.1% of total budget
Minor	2	0.1% < x =< 0.5% of total budget
Moderate	3	0.5% < x =< 1 of total budget
Major	4	1% < x =< 2% of total budget
Severe	5	x > 2% of total budget

Source: Research Data

Table 3. Performance impact criteria example

Impact	Value	Explanation
Insignificant	1	Performance drop < 20%
Minor	2	20% < Performance drop < 40%
Moderate	3	40% < Performance drop < 60%
Major	4	60% < Performance drop < 80%
Severe	5	Performance drop > 80%

Source: Research Data

Table 4. Risk analysis matrix example

		Impact	1	2	3	4	5
Likelihood			Insignificant	Minor	Moderate	Major	Severe
5	Almost certain	1	9	15	18	23	25
4	Likely	2	6	12	16	19	24
3	Moderate	3	4	10	14	17	22
2	Unlikely	4	2	7	11	13	21
1	Rare	5	1	3	5	8	20

Source: Research Data

Table 5. Risk level and action plan

Risk Level	Risk Value	Action
Insignificant	20-25	Immediate action is required to manage risks
Minor	16-19	Action is required to manage risk
Moderate	12-15	Action is taken if resources are adequate
Major	6-11	Action taken if necessary
Severe	1-5	No action required

Source: Research Data

Risks are categorized from very high (20–25, immediate action needed) to very low (1–5, no action needed) as shown in Table 8. Regular reviews ensure appropriate actions are taken. Using all the instruments defined previously, a risk assessment can be conducted. The results of the risk assessment for KNEKS are presented in Table 9. The top ten identified risks for KNEKS include natural disasters, terrorism, data loss, and hardware damage. These top risks are further assessed for their impact to identify which entities might be affected. Table 10 outlines the entities affected by each of the risks.

The likelihood and impact values in the risk assessment were assigned collaboratively by the research team in consultation with the KNEKS IT Division Head and two system administrators during structured assessment workshops. Each risk item was discussed and scored based on organizational experience, historical incident data, and the professional judgment of the informants. Consensus was reached through deliberation, and where disagreements arose, the average of individual scores was adopted as the final value.

Table 6. KNEKS risk assessment

Likelihood Level	Value	Likelihood Criteria		
		Likelihood	Impact	Value
Natural Disaster	Flood	1	3	5
	Storm	1	3	5
	Tsunami	1	5	20
	Earthquake	2	5	21
	Fire	2	5	21
Man-Made Disasters	Theft	2	2	7
	Sabotage	2	2	7
	Dispute	2	2	7
	Terrorism	2	5	21
	Civil unrest	2	5	21
Infrastructure Failure	Building specific errors	1	3	5
	Failure of non-ICT equipment	1	3	5
	Electrical failure	1	4	8
IT Specifics	Data is lost or damaged	2	5	21
	Data backup failure	1	5	20
	Virus attacks, worms, malware	3	4	17
	Hacker/cracker attacks	3	4	17
	Hardware damage	2	5	21
	Use of non-original software	1	2	3
	Insufficient internet connection	4	3	16
	Network connection lost	2	4	13
	Documentation or procedures for using the program/application are incomplete	3	2	10
	Unscheduled maintenance	4	1	6
	ICT management capabilities	3	3	14
	The program/application interface is difficult to understand	4	2	12
	Organizational data leaks	1	1	1
	SOP violation	3	2	10
	Lack of understanding of the rules	3	2	10
	Server down	3	3	14
	Server condition is inadequate	2	2	7
	The device is overheating/overloading	2	2	7
	Stakeholder understanding is inadequate	3	2	10

Source: Research Data

After doing risk assessments, Business Impact Analysis (BIA) evaluates critical applications' downtime tolerance and security categories. For KNEKS:

1) Currently managed applications have moderate to low criticality
2) Third-party applications have higher criticality

The BIA process assesses:

1) Critical business processes.
2) Recovery needs.

3) Security categories (using FIPS 199: low, moderate, high).

Key downtime metrics include:

1) Maximum Tolerable Downtime (MTD).
2) Recovery Time Objective (RTO).
3) Recovery Point Objective (RPO).

Table 7. Affected Entities

Risk	Risk Impact	Affected Entities
Natural Disaster	The office space was destroyed	Office room
	Staff cannot access the office	Staff
	Electrical constraints	Electricity
	Information systems are destroyed	System
	Hardware damage	Working tool
	Data center meltdown	Data center
Terrorism and riots	Staff cannot access the office	Staff
	Hardware damage	Working tool
Management failure	Data loss	Data
	Application failure	Application
	Hardware damage	Working tool
ICT attacks from outside	The information system is down	System
	Data theft	Data
	Data loss	Data
	The company's good name is tarnished	Reputation

Source: Research Data

Figure 1 illustrates the relationship between business processes and applications, along with their downtime metrics and their security impacts in terms of confidentiality, integrity, and availabity. Separating the internal systems and external systems would help KNEKS in the strategizing phase of DRP.

Controls

Based on the impacts identified in the BIA, KNEKS should implement appropriate preventive measures and controls. NIST SP 800-53 should be helpful to find suitable controls for thos entities. These should be designed to mitigate identified risks and reduce potential impact on critical business processes.

Recovery Strategy

KNEKS must develop strategies to mitigate threats to critical information systems and business processes. Key components of the recovery strategy include:

Backup and recovery strategies should be designed based on the allowable downtime determined in the BIA. For KNEKS:

1) Low-impact systems: Regular daily or weekly backups using offsite or cloud storage.
2) High-priority systems: More advanced strategies such as real-time backup, encrypted offsite storage, or mirrored systems from third-party services with SLAs.

For backup methods, KNEKS should establish clear policies defining minimum backup frequency, data scope, storage location, file naming conventions, media rotation frequency, and transfer methods to offsite storage. An initial implementation should start with a backup SOP, improving upon the current system administrator-managed backups.

To ensure business continuity during major system failures, KNEKS should consider these followings regarding alternative data processing sites:

1) Geographic separation of data storage sites.
2) Establishing a cold site (data storage only) initially.
3) Planning for potential upgrade to warm or hot sites as the organization grows.

The proposed recovery strategy aligns with the recommendations of NIST SP 800-34 and is consistent with previous studies emphasizing the importance of backup redundancy and alternative processing facilities as key determinants of organizational resilience (Ashrafi & AlKindi, 2022; Supriyanto et al., 2019). However, unlike previous studies that primarily focused on established enterprise environments, this study proposes a phased implementation model that allows KNEKS to gradually transition from basic backup arrangements toward more advanced disaster recovery infrastructure as organizational capacity and PDES maturity increase. This finding highlights the importance of aligning disaster recovery investments with institutional growth trajectories rather than adopting a one-size-fits-all implementation approach.

Recovery Procedures

The DRP included emergency procedures for the Recovery Team to restore systems and support facilities. These procedures covered: activation and notification phase, recovery phase, and reconstitution phase. Each phase detailed specific steps, responsibilities, and escalation procedures.

The activation and notification phase should follow these following steps:

1) Detect and report the incident.
2) Assess the situation and determine if it meets disaster criteria.
3) Notify key personnel.
4) Declare a disaster if criteria are met.
5) Activate the Disaster Recovery Team.

Responsibilities in the activation and notification phase:

1) First Responder: Detect and report the incident.
2) Team Leader: Assess the situation, declare disaster if necessary.
3) Recovery Coordinator: Notify key personnel, activate DR Team.

Escalation Procedures in the activation and notification phase:

1) If the Team Leader is unavailable, the Recovery Coordinator assumes authority.
2) If the incident severity increases, escalate to executive management.

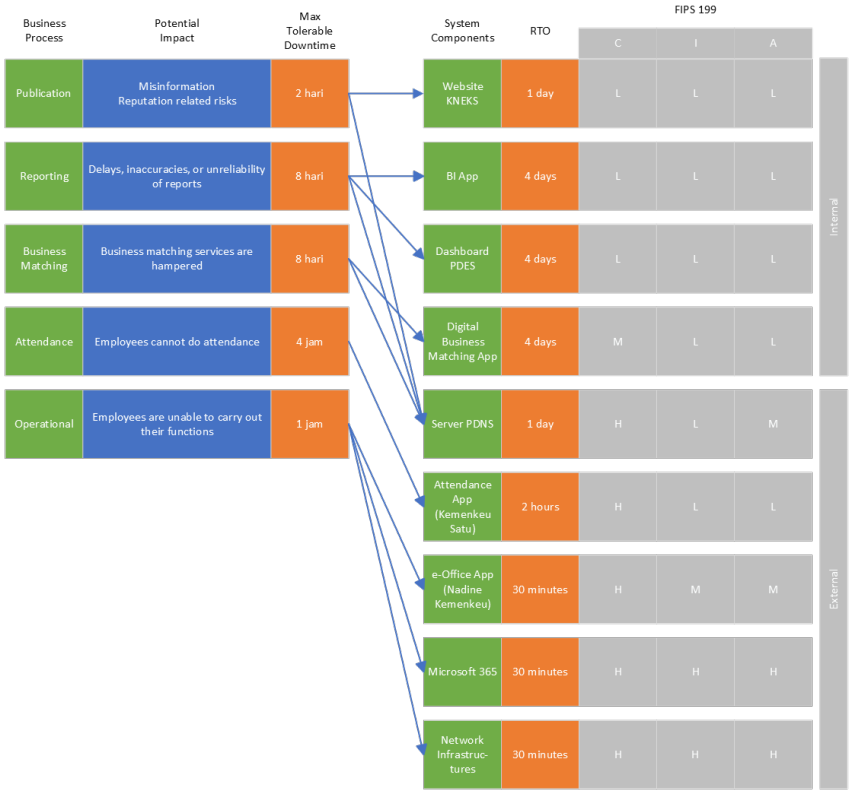

Figure 1. KNEKS business impact analysis
Source: Research Data

Figure 1 illustrates the comprehensive mapping of KNEKS's business processes to their supporting applications, categorized into internally managed and externally hosted systems. The diagram presents the downtime metrics (MTD, RTO, RPO) for each application alongside their FIPS 199 security impact categorization across confidentiality, integrity, and availability dimensions. This visual representation enables KNEKS to identify which systems require the most stringent recovery procedures and informs the prioritization of recovery efforts during disaster response.

The recovery phase should follow these following steps:

1) Conduct detailed damage assessment.
2) Prioritize recovery activities based on BIA.
3) Activate alternative processing sites (if necessary).
4) Restore critical systems and data.
5) Verify functionality of restored systems.
6) Resume business operations.

Responsibilities in the recovery phase:

1) Disaster Assessment Team: Conduct damage assessment.
2) Recovery Coordinator: Prioritize activities, oversee recovery process.
3) Network Recovery Team: Restore network infrastructure.
4) Server Recovery Team: Restore server functionality.
5) Backup & Restore Team: Recover data from backups.
6) Application Recovery Team: Restore critical applications.

Escalation Procedures in the recovery phase:

1) If recovery of a critical system fails, escalate to Team Leader.
2) If recovery time exceeds RTO, escalate to executive management.

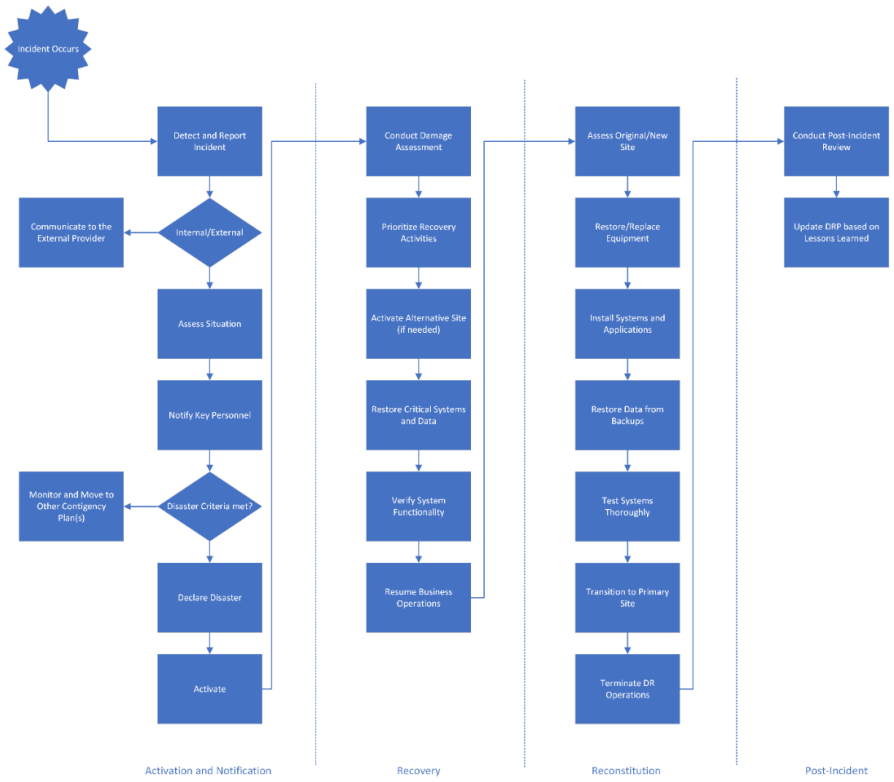

Figure 2. High-Level Recovery Procedures
Source: Research Data

Figure 2 provides a high-level overview of the three-phase recovery procedure workflow, depicting the sequential flow from incident detection through activation, recovery operations, and reconstitution back to normal operations. The diagram highlights decision points, escalation triggers, and the handoff responsibilities between recovery teams at each phase transition.

The reconstitution phase should follow these following steps:

1) Assess the original or new site for operations.
2) Restore or replace affected equipment.
3) Install systems and applications.
4) Restore data from backups.
5) Test systems thoroughly.
6) Transition operations from alternative site to primary site.
7) Terminate disaster recovery operations.

Responsibilities in the reconstitution phase:

1) Team Leader: Oversee reconstitution process.
2) Recovery Coordinator: Coordinate transition of operations.
3) All Recovery Teams: Restore respective systems and conduct testing.
4) Communication Team: Notify stakeholders of return to normal operations.

Escalation Procedures in the reconstitution phase:

1) If issues arise during reconstitution, escalate to Team Leader.
2) If significant delays occur, escalate to executive management

Regular Testing

KNEKS should implement a comprehensive testing program, including:

1) Development of test plans,
2) Personnel training, and
3) Regular drills and exercises.

Initially, KNEKS should focus on instruction or discussion-based training before progressing to larger-scale functional training.

Maintenance Plan

To ensure the DRP remains effective, KNEKS must:

1) Regularly update the plan to reflect changes in systems, procedures, organizational structure, and policies.
2) Conduct reviews after significant organizational changes.
3) Frequently review and update the contact list.
4) Focus reviews on operational needs, security requirements, technical procedures, hardware, software, and other equipment.

Key Findings

The study has explored several components for each process using guidelines such as ISO 31000, NIST SP 800-53, and NIST FIPS 199. Based on KNEKS's current needs and conditions, a DRP framework has been formulated, as presented in Figure 2. It's important to note that DRP is a continuous process that needs regular review and updates to match the organization's evolving goals and needs.

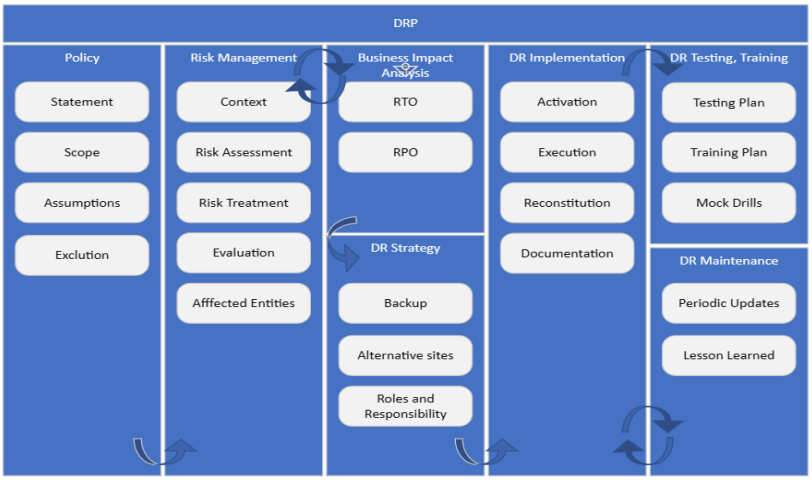

Figure 3. Reccomened DRP Framework for KNEKS
Source: Research Data

CONCLUSION

This study assessed the disaster recovery readiness of the National Committee for Sharia Economics (KNEKS) and developed a Disaster Recovery Plan (DRP) framework based on NIST SP 800-34 to support the future development of the Sharia Economic Data Center (PDES). The findings indicate that KNEKS possesses several fundamental disaster recovery capabilities, particularly in backup management, recovery prioritization, alternative storage arrangements, and communication coordination. However, the maturity assessment and gap analysis reveal significant deficiencies in activation procedures, reconstitution planning, testing programs, system redundancy, and coordination with related continuity plans. These findings suggest that while basic operational resilience mechanisms are in place, a structured and formalized disaster recovery governance framework has not yet been fully established.

This study contributes to the disaster recovery planning literature by demonstrating the applicability of NIST SP 800-34 in an emerging public-sector institution undergoing digital transformation and data center development. The proposed maturity- and gap-based implementation approach provides a practical mechanism for prioritizing DRP development according to organizational readiness and resource availability. Nevertheless, this study is limited to a single case study and relies on assessments obtained from a limited number of key informants. Furthermore, the proposed framework has not yet been evaluated through full-scale disaster recovery testing. Future studies are therefore encouraged to conduct comparative investigations across multiple public-sector institutions and evaluate the effectiveness of the framework through implementation and simulation-based validation.

ACKNOWLEDGEMENT

The authors express sincere gratitude to Bina Nusantara University for providing institutional support and research facilities that made this study possible. The authors also extend their appreciation to the National Committee for Sharia Economics (KNEKS) for granting access to organizational data, facilitating interviews with key stakeholders, and providing valuable feedback during the framework development process.

AUTHOR CONTRIBUTION STATEMENT

Khalil Mojadidi contributed to the conceptualization of the study, data collection, data analysis, framework development, and preparation of the original manuscript draft. Abba Suganda Girsang contributed to research supervision, methodology validation, critical review and editing of the manuscript, and overall guidance throughout the research process. Both authors have read and approved the final version of the manuscript and agree to be accountable for all aspects of the work.

REFERENCES

Ahmad, A., Alshurideh, M., Al Kurdi, B., Aburayya, A., & Hamadneh, S. (2021). Digital transformation metrics: a conceptual view. *Journal of Management Information and Decision Sciences*, *24*(7), 1–18.

Al Hassan, L. K. M. (2017). *Information technology disaster recovery plan (IT DRP) framework–A study on IT continuity for smart city in Abu Dhabi smart government*. The British University in Dubai.

Alifian, M. H., & Priharsari, D. (2021). Penyusunan Disaster Recovery Plan (DRP) menggunakan framework NIST SP 800-34 (Studi kasus pada perusahaan IT Nasional). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *5*(10), 4673–4679. https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/10056

Almutawa, E. (2026). *An investigative study into operational leadership's disaster recovery (DR) planning at Dubai Civil Defence (DCD).* University of Gloucestershire.

Arroyo-Melendez, A. E. (2026). *Better IT Disaster Recovery and Procedures to Improve Response After Computer Crime*. Walden University.

Ashrafi, R., & AlKindi, H. (2022). A framework for IS/IT disaster recovery planning. *International Journal of Business Continuity and Risk Management*, *12*(1), 1–21. https://doi.org/10.1504/IJBCRM.2022.121645

Cedergren, A., Hassel, H., & Vallin, L. (2026). The Cost of Adaptability: Exploring the Dual Nature of Adaptive Capacity Through a Healthcare Case Study. *Journal of Contingencies and Crisis Management*, *34*(2), e70178.

Craven, E., & Tomlinson, S. (2026). Contingency planning in farm practice. *In Practice*, *48*(1), 8–17.

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). SAGE Publications.

Dearniwati, E., Nurlette, G. A., Anwar, S., & Purwanto, H. (2025). Preparation of IT Disaster Recovery Plan (DRP) using NIST SP 800-34 Framework (Case Study: PT Pamapersada Nusantara, Jakarta). *Eduvest-Journal of Universal Studies*, *5*(1), 954–962.

Dwi Pamungkas, E., Fatonah, N. S., Firmansyah, G., & Akbar, H. (2023). Disaster Recovery Plan analysis based on the NIST SP 800-34 framework (Case study: PT Wijaya Karya (Persero) Tbk.). *Jurnal Indonesia Sosial Sains*, *4*(9), 936–947. https://doi.org/10.59141/jiss.v4i09.879

Epstein, B., & Khan, D. C. (2014). Application impact analysis: A risk-based approach to business continuity and disaster recovery. *Journal of Business Continuity & Emergency Planning*, *7*(3), 230–237.

Ferrer, J. P., & Mandigma, M. B. S. (2026). Relationship of Perceived Organizational Support and Organizational Commitment on the Business Continuity Management of Selected Philippine Financial Shared Services Companies. *Review of Integrative Business and Economics Research*, *15*(3), 459–476.

Hassel, H., & Cedergren, A. (2021). Integrating risk assessment and business impact assessment in the public crisis management sector. *International Journal of Disaster Risk Reduction*, *56*, 102136. https://doi.org/10.1016/j.ijdrr.2021.102136

Hendaryatna, H., Firmansyah, G., Tjahjono, B., & Widodo, A. M. (2023). Performance evaluation of business continuity plan in dealing with threats and risks in Cilegon companies use ISO 22301:2019 & NIST SP 800-30 R1 frameworks case study: PT. X. *Asian Journal of Social and Humanities*, *1*(12), 1159–1174. https://doi.org/10.59888/ajosh.v1i12.120

Kesa, D. M. (2023). Ensuring resilience: Integrating IT disaster recovery planning and business continuity for sustainable information technology operations. *World Journal of Advanced Research and Reviews*, *18*(3), 970–992.

Lubis, M., Luthfi, M. I., Saedudin, R. R., Muttaqin, A. N., & Lubis, A. R. (2026). The Integration of ISO 27005 and NIST SP 800-30 for Security Operation Center (SOC) Framework Effectiveness in the Non-Bank Financial Industry. *Computers*, *15*(1), 60.

Mohamed, H. (2014). A proposed model for IT disaster recovery plan. *International Journal of Modern Education and Computer Science*.

Rambharose, R. (2026). Theorising Recognition of Prior Learning Research in Higher Education: A Multidisciplinary Framework for Qualitative, Quantitative, and Mixed-Methods Inquiry. *International Journal of Qualitative Methods*, *25*. https://doi.org/10.1177/16094069251404325

Saleem, K. (2008). *Towards a business continuity information network for rapid disaster recovery*.

Sawalha, I. H. (2021). Views on business continuity and disaster recovery. *International Journal of Emergency Services*, *10*(3), 351–365.

Singh, A., & Alshammari, M. (2023). Advancing, empowering, and reshaping Saudi society through integrating e-learning technology into higher education. *Int. J. Adv. Appl. Sci*, *10*, 178–187.

Singh, H. P., Alshammari, K., & Singh, H. P. (2021). Impacts of Digital technology-enabled personalized and adaptive learning on student learning performance: A TOE framework for Saudi Arabia. *& Applied Sciences & Technologies*, *12*(13), 1–12.

Snedaker, S. (2013). *Business continuity and disaster recovery planning for IT professionals*. Newnes.

Stamenkov, G. (2025). Cloud service models, business continuity and disaster recovery plans, and responsibilities. *International Journal of Organizational Analysis*, *33*(3), 437–451. https://doi.org/10.1108/IJOA-12-2023-4127

Supriyanto, A., Aknuranda, I., & Putra, W. H. N. (2019). Penyusunan Disaster Recovery Plan (DRP) berdasarkan framework NIST SP 800-34 (Studi kasus: Departemen Teknologi Informasi PT Pupuk Kalimantan Timur). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*,

3(8), 8212–8219. https://j-ptiik.ub.ac.id/index.php/j-ptiik

Suresh, N. C., Sanders, G. L., & Braunscheidel, M. J. (2020). Business continuity management for supply chains facing catastrophic events. *IEEE Engineering Management Review*, *48*(3), 129–138.

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). Contingency planning guide for federal information systems. *NIST Special Publication*, 800–834.

Tatineni, S. (2023). Cloud-based business continuity and disaster recovery strategies. *International Research Journal of Modernization in Engineering, Technology, and Science*, *5*(11), 1389–1397.