Journal of Sisfotek Global

Versi Online: http://journal.stmikglobal.ac.id/index.php/sisfotek
ISSN (Online): 2721 - 3161, ISSN (Print): 2088 – 1762
Vol. 11, No. 2, September 2021, pp. 75-81

Designing a Disaster Recovery Plan Using NIST 800-34 Framework on the Information System of The Directorate General of Hajj and Umrah

[1]Nurhanudin

[1]Young Expert Computer Provisions / Directorate General of Hajj and Umrah, Ministry of Religion
E-mail: [1]nurhanudin@kemenag.go.id

ARTICLE HISTORY

Received : 18 August, 2021
Revised : 3 September, 2021
Accepted : 15 September, 2021

KEYWORDS

Information System
Disaster Recovery Plan
NIST 800-34
Hajj and Umrah

ABSTRACT

The Directorate General of Hajj and Umrah manages an information system that is used to provide services in the business process of organizing Hajj and Umrah, the services provided include registration, cancellation, settlement, portion assignment, hajj document management, embarkation operations, Saudi Arabia operations, and debarkation operations. The services are provided throughout the year, thus requiring infrastructure support and adequate information systems that can run24 hours a day. To maintain and ensure the continuity of Hajj and Umrah services, a Disaster Recovery Plan is designed, which is used as a guide in dealing with disasters or disturbances that can occur at any time and can disrupt all operational activities of the organization. In this study, the NIST 800-34 framework is used, starting with risk identification and assessment, Business Impact Analysis (BIA), preventive controls identification, contingency strategies, and contingency plans. The contingency plan preparation phase includes the activation phase, the recovery phase, and the reconstitution phase. Based on the result of research, there are ten risks that can threaten the continuity of information system services and based on Business Analysis Impact, services with a high critical level are Siskohat and Haji Pintar applications. The research produced is in the form of a Disaster Recovery Plan document that is adapted to the organizational conditions of the Directorate General of Hajj and Umrah**.**

1. INTRODUCTION

The Directorate General of Hajj and Umrah is the implementing element under and responsible to the Minister of Religion, who has the task of carrying out the formulation and implementation of policies in organizing Hajj and Umrah following with the provisions of laws and regulations [1]. Currently, information technology is widely used in all fields had impacted on increasing the quality and performance of an organization [2], one of which is used in the organization of Hajj and Umrah where the Directorate General of Hajj and Umrah builds an information system to serve hajj and umrah pilgrims. The Directorate General of Hajj and Umrah manages the information system used to support the operational business processes of the hajj and umrah organization. One of the information systems used is the Integrated Hajj Computerized System, hereinafter referred to as Siskohat, which is an integrated data and information management system for the implementation of hajj [3]. Siskohat operates 24 hours for continuous service, Siskohat integrates all services in the business process of organizing hajj and umrah starting from registration, cancellation, settlement, portion assignment, hajj document management, embarkation operations, Saudi Arabia operations, and debarkation operations. Management of information and data is carried out continuously to ensure the security, accuracy, and integrity of the resulting data [4], considering that data and information are precious assets [5] for an organization as an absolute requirement whether the organization can run well [6].

Information and data are essential for organizations to carry out daily activities in providing services to the community, but currently there is no operational plan mitigation that is used in the event of a disaster so that organizations can cause losses, including information that cannot be accessed (loss of

availability), data is corrupted or data has been damaged (loss of integrity), and there is a leak of important information that should be protected [7]. This can lead to a decrease in an organization's reputation for maintaining the accuracy, availability, and security of information and data.

These problems can be formulated by providing solutions on how to design mitigation of information system management in the event of a disaster by creating a Disaster Recovery Plan document which is an important part of maintaining information and data so that they can be accessed and services run as they should [8]. The Disaster Recovery Plan has been widely applied to organizations, both universities, private, and government agencies on how to save important information and data.

Research at the Sriwijaya State Polytechnic related to the design of an academic information system Disaster Recovery Plan using the NIST 800-34 framework, where this research resulted in a Disaster Recovery Plan document against nine threats and eight POLSRI SISAK sub-systems with stages starting from problem determination, goal setting, data collection , data verification, risk management, preparation of draft Disaster recovery Plan, validity of draft Disaster Recovery Plan, and determination of Disaster Recovery Plan documents [9].

Another research at the University of Muhammadiyah Sukabumi related to the implementation of the NIST 800-34 framework in the design of an academic information system Disaster Recovery Plan where the research stages started from problem determination, data collection, asset identification and assessment, risk assessment, business impact analysis which resulted in a system that had an impact. The largest is the Student Finance System with a percentage value of 99%, while the sub-system that has the lowest score is the Academic Guidance System with a percentage value of 62% [10].

Research related to the information technology recovery plan strategy conducted in universities using the NIST 800-34 framework with the stages of risk assessment, business impact analysis, recovery strategy, testing, and plan documentation shows that the Disaster Recovery Plan document can help restore information systems in the event of a disaster. Based on the priority level of impact risk where the highest impact is Website Student with a score of 100% [11].

This research will design a Disaster Recovery Plan for information systems at the Directorate General of Hajj and Umrah using the NIST 800-34 framework released by the National Institute of Standards and Technology [12]. The purpose of preparing the Disaster Recovery Plan is to record all information related to the Directorate General of Hajj and Umrah to deal with disasters and document the steps that must be taken in the event of a disaster.

2. METHODS

The research method carried out is guided by the NIST 800-34 framework, which is adapted to the conditions and needs of the organization with the flow as shown in Figure 1.

1. Risk Identification and Assessment

At this stage, doing identification of risks that may occur, both controllable and uncontrollable, and doing a risk assessment on threats had impacted on disrupting the information system services. The result of this stage is which the threats including controllable and uncontrollable risks and assesses the threats that occur, vulnerability, critical assets (office and building assets) and consequence: operational stop, damage the facility (electrical, equipment, and networks) or slows down system performance.

2. Business Impact Analysis (BIA)

The stage of analyzing which business processes or information systems have the greatest impact in the event of a disaster that can disrupt the organization's operations.

3. Identification of Preventive Controls.

Identify information systems that have a high level of risk in order to get more attention to minimize the impact of risks that occur.

4. Preparation of Contingency Strategies

This stage Determines backup strategies and alternative locations so that information system services can run properly.

5. Preparation of Contingency Plan

the stage of preparing a contingency plan which consists of 3 phases, namely the activation phase, the recovery phase and the reconstruction phase in dealing with disasters.

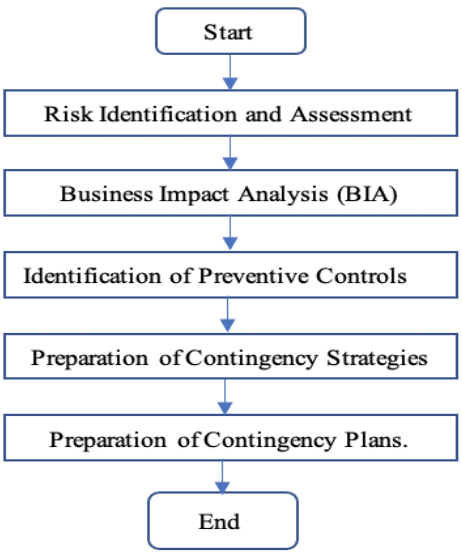


Figure 1. Flow of Research

3. RESULTS AND DISCUSSION

3.1. Risk Identification and Assessment

1. Risk Identification

The identification process includes risks that are within and beyond the organization's control. This identification is carried out in detail so that risk sources, causes, and risk control can be recognized and carried out correctly. The results of identifying of risks that can disrupt the process of information system services at the Directorate General of Hajj and Umrah are shown in Table 1.

Table 1. Kind of risk that can disrupt the process of information system

No	*Threat*	*Control/Uncontrol*
1	Earthquake	Uncontrol
2	Fire	Uncontrol
3	Flood	Uncontrol
4	Lightning	Uncontrol
5	Volcanic eruption	Uncontrol
6	Electricity failure	Uncontrol
7	Human error	Control
8	Server down	Control
9	Cyber attack	Control
10	Virus, malware	Control

2. Risk Assessment

Risk assessment is carried out to assess the level of risk that may occur in the information system. This risk can be mitigated by suppressing the vulnerabilities factor or reducing the impact of the risk [13]. In this research, a risk assessment assesses the potential risks in the information system used for the business process services to implement of hajj and umrah. One of the references that become parameters in the risk assessment is the results of field observations, where data on events, such as technical problems, hacker attacks, or fires. Risks that occur either completely or only partially can disrupt the operation of information systems, such as electricity failures, earthquakes, floods, fires, volcanic eruptions, server damage, virus attacks, and others. According to observation data, there has been a power outage at the Siskohat Building, resulting in information system services not running and some hardware failures such as personal computers, UPS, and backup devices. The Risk Assessment stage is the first stage of the Disaster Recovery Plan procedure. Risk assessment is used to determine what threats have the potential to pose a risk to the information system at the Directorate General of Hajj and Umrah. Table 2 describes the threats that may pose a risk along with data on vulnerabilities, critical assets, and the consequences of the threats.

Table 2. Risk assessment

No	*Threat*	*Threat that occur*	*vulnerability*	*Critical assets*	*Consequence*
1	Earthquake	An earthquake can damage existing infrastructure in a building if it exceeds a magnitude of 5 on the Richter scale	Infrastructure is located in buildings that can only withstand earthquakes up to 5 on the Richter scale	Office and building assets	Operational stop
2	Fire	All types of activities that cause electrical sparks and short circuits or fires from outside the building	Flammable material	Office and building assets	Operational stop
3	Flood	Floods can cause damage to office facilities and infrastructure	damage to office facilities and infrastructure	Office and building assets	Operational stop
4	Lightning	Lightning strikes can cause damage to the electrical network or LAN and electronic devices	Lightning can hit servers causing damage to organization assets	Office and building assets	Operational stop
5	Volcanic eruption	Lava and ash from volcanic eruptions can disrupt and even stop operations	All employees must be evacuated and operational activities stop	Office and building assets	Operational stop
			Equipment that requires		

			electricity does not work		
6	Electricity failure	Electricity failure can cause hardware failure	Deleted data, data input error	Computers and office assets	Damage to electrical equipment and networks
			Unable to process request	Information and data	
7	Human error	Human error can lead to loss of information and data	Vulnerabilities can still be penetrated by hackers	Information and data	Operational stop
8	Server down	The high traffic causes the server to go down	Vulnerabilities due to antivirus not being updated or not turned on	Information and data	Operational stop
9	Cyber attack	Attacks and threats for example Phishing, Sniffing, SQL Injection, defacing, DDoS, or Backdoor			Operational stop
				Information and data	
10	Virus, malware	Disruption of system or network activity because it has been infected with a virus or malware through servers, routers and ends user computers.			Slows down system performance, can stop and damage the system and data

3.2. Business Impact Analysis (BIA)

Business impact analysis is a stage in making a Disaster Recovery Plan which is carried out to find out which business processes are vital business processes within the organization and also to find out the impact that the organization will experience in the event of a disruption or disaster in the information system that supports its business processes [14]. Business Impact Analysis aims to assist an organization in understanding the impact of an unexpected disaster. So it takes a tolerable time if a service stops operating. Mapping information system services can be done to determine what services an information system provides to both internal organization and the community and determine the critical level of the information system. There are 3 categories of critical levels of disruption or disaster impact on information systems, that is:

1. High

Information systems have significant impacts and side effects on the institution and the sustainability of an organization in addition to having an impact on outside parties or system.

2. Medium

Information systems affect the main activities of each work unit in an organization and have a severe impact on the organization.

3. Low

The information system only impacts on organization support activities or is only used within the internal scope of a small organization.

Table 3 shows the impact obtained if the existing information system at the Directorate General of Hajj and Umrah is disrupted and explains the level of impact on business.

Table 3. Kind of risk that can disrupt the process of information system

No	*Information system*	*Impact if down*	*Impact level*
1	Siskohat	Hajj business process cannot be accessed	High
2	Siskopatuh	Umrah business process cannot be accessed	Medium
3	Haji Pintar	Public information services cannot be accessed	High
4	Umrah Cerdas	Public information services cannot be accessed	Medium
5	Sepakat	System cannot be accessed	Low

3.3. Identification of Preventive Controls

Preventive control is made so that information systems that have identified and assessed risks and made business impact analysis get attention according to the level of risk and have standard control procedures to reduce/minimize the impact of risks that occur. From the business impact analysis results, it is known that the systems that have a high level of risk are Siskohat and the Haji Pintar Application, this is

because these systems are used for continuous services that internal and external users access.

3.4. Preparation of Contingency Strategies

Contingency strategy is focused on determining backup strategy and alternative locations of information system services.

1. Backup Strategy

The recommended backup strategy for information system services at the Directorate General of Hajj and Umrah is related to the backup method, the frequency of backups and the type of backup that can be carried out with consideration of information and data that can be tolerated in the event of disruption/damage.

2. Alternative Location

The recommended alternative location is the Disaster Recovery Center of the Directorate General of Hajj and Umrah, which is located in Surabaya. Alternative locations are used when the condition of infrastructure and information systems due to a disaster suffers significant damage that cannot be recovered in a short time. To assess the level of damage that occurred to the Data Center due to a disaster, the Disaster Recovery Planning team was carried out. The assessment results were reported to the Disaster Recovery Lead for decision making.

3.5. Preparation of Contengency Plans

Following the NIST 800-34 framework, there are three phases carried out in forming a contingency plan, namely the activation phase, the recovery phase, and the reconstitution phase. In the event of a disaster, it is hoped that the Disaster Recovery Plan Team can carried out all phases. The Disaster Recovery Plan Team of the Directorate General of Hajj and Umrah consists of:

- Disaster Recovery Lead
- Disaster Management Team
- Facility Team
- Network and Server Team
- Application Team
- Operational Team
- Leader Team
- Communication Team

Each team has its duties and responsibilities and designing the Disaster Recovery Plan also includes media handling, assembly points and relocation to alternative locations.

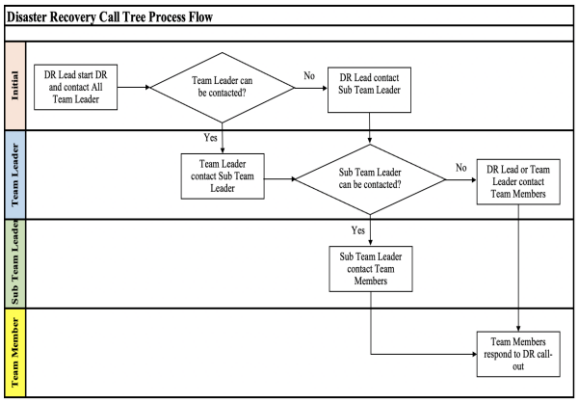
1. Activation Phase

After a disaster is declared, the DR Lead must start activating the Disaster Recovery Plan by performing the DR Call Tree procedure. After the DR Lead officially declares that a disaster has occurred, the DR Lead will start the activation of the Disaster Recovery Plan by running a DR Call Tree. The information provided in the DR Call Tree which is carried out by the DR Lead and forwarded to the next level is:

- That a disaster has occurred;
- Nature of the disaster (if known);
- Initial estimate of the magnitude of the disaster (if known);
- Initial estimate of the impact of the disaster (if known);
- Initial estimate of the estimated duration of the disaster (if known);
- Actions taken;
- Actions to be taken before to the DR Lead and Team meeting;
- Scheduled meeting place for DR Lead and Team meeting;
- Scheduled meeting times for DR Lead and Team meetings;
- Other related information.

The flow of the Disaster Recovery Call Tree process is as shown in Figure 2.

Figure 2. Disaster recovery call tree process flow



2. Recovery Phase

This phase is carried out when the Disaster Recovery Plan has been activated and the DR Lead has announced the occurrence of a disaster so that information system service operations run on standby facilities/alternative locations which are Disaster Recovery Centers for some time. When the information system service runs on a standby facility, recovery is carried out at the main facility / Data Center to repair damage to infrastructure and information systems due to a disaster by carrying out a criticality rating – system one procedure. The

recovery flow is shown in Figure 3.

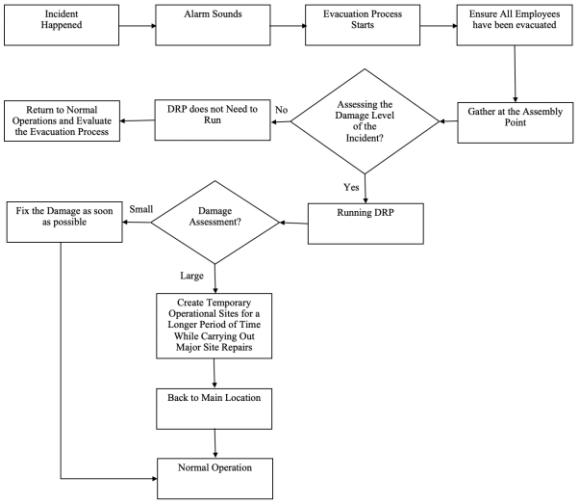


Figure 3. Recovery flow

3. Reconstitution Phase

After the recovery is complete, the next phase is the reconstitution phase, which is a phase that focuses on validating the recovery process and deactivating the Disaster Recovery Plan. The activities carried out in this phase are:

- Concurrent processing;
- Data validity test;
- Function validity test;
- Cleanup
- Offsite data storage;
- Data backup;
- Documentation;
- Disaster Recovery Plan deactivation.

4. CONCLUSIONS

There are ten risks can threaten the continuity of information system services at the Directorate General of Hajj and Umrah, these risks can be controlled and cannot be controlled, risks that can be controlled by humans such as human error or virus attacks, while the risks that cannot be controlled are risks caused by due to natural disasters.

Based on Business Analysis Impact, services with a high critical level are Siskohat and Haji Pintar applications, medium critical levels are Siskopatuh and Umrah Cerdas applications, while those with a low critical level are Sepakat.

Disaster Recovery Plan at Directorate General of Hajj and Umrah consists of several teams coordinated by DR Lead who can decide on Disaster Recovery Plan activation when a disaster occurs. This Disaster Recovery Plan is divided into three phases: the activation phase, the recovery phase, and the reconstitution phase.

The Disaster Recovery Plan design is equipped with recovery flow templates / forms, damage assessment forms, disaster event logs, recovery activity logs, Disaster Recovery team mobilization logs, Disaster Recovery Progress, and Recovery Completion Functions, so the Disaster Recovery Plan document becomes a reference for standard operating procedures in dealing with disasters.

REFERENCE

[1] Kementerian Agama Republik Indonesia, “Peraturan Menteri Agama Republik Indonesia Nomor 42 Tahun 2016 tentang Organisasi dan Tata Kerja Kenenterian Agama”, Indonesia, 2016

[2] Dedi, A. Sidik, M. Raya, M.B. Ryando, “Perancangan Sistem Informasi Promosi Jasa Foto dan Studio Musik pada M2N Studio *Production*”, Jurnal Sisfotek Global, vol. 11, no. 1, pp. 48-52, Maret 2021

[3] Pemerintah Republik Indonesia, “Undang-Undang Republik Indonesia Nomor 8 Tahun 2019 tentang Penyelenggaraan Ibadah haji dan Umrah”, Indonesia, 2019

[4] R.E. Indrajit, “Konsep dan Strategi Keamanan Informasi di Dunia Cyber”, Yogyakarta: Graha Ilmu, 2014

[5] R. Budiarto, “Manajemen Risiko Keamanan Sistem Informasi”, Journal of Computer Engineering System and Science, vol. 2 (2), pp. 48-58, 2017

[6] Yakub, “Pengantar Sistem Informasi”, Yogyakarta: Graha Ilmu, 2012

[7] M.E. Whittmen, H.J. Mattord, “Management of Information Security Fourth Edition”, Course Technology Cengage Learning, Stamford, 2013

[8] S.R. Wicaksono, “Disaster Recovery Planning”, Jakarta: Seribu Bintang, 2009

[9] M.Z. Agung, “Perancangan Disaster Recovery Plan Sistem Informasi Akademik dengan Pendekatan Kerangka Kerja NIST 800-34”, Jurnal teknologi Rekayasa, vol. 4, no. 2, hal. 157-166, Desember 2019

[10] I.G.T. Isa, “Implementasi Pendekatan Kerangka Kerja NIST 800-34 dalam Perancangan Disaster Recovery Plan pada Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi”, Jurnal Ilmiah Ilmu Komputer, vol. 15, September 2020

[11] D. Suhartono, K.N. Isnaini, “Strategi Recovery Plan Teknologi Informasi di Perguruan Tinggi Menggunakan Framework NIST SP 800-34”, Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer, vol. 20, no. 2, pp. 261-272, Mei 2021

[12] The website NIST (Online), Available: https://csrc.nist.gov

[13] Gibson, “Managing Risk in Information System, 2nd Edition” USA: Jones & Bartlett Learning, 2014

[14] R.L. Tammineedi, “Business Continuity Management: A Standars-Based Approach”