Eduvest – Journal of Universal Studies
Volume 5 Number 1, January, 2025
p- ISSN 2775-3735- e-ISSN 2775-3727

PREPARATION OF IT DISASTER RECOVERY PLAN (DRP) USING NIST SP 800-34 FRAMEWORK (CASE STUDY: PT PAMAPERSADA NUSANTARA, JAKARTA)

Erma Dearniwati[1], Gusti Ahmad Nurlette[2], Saiful Anwar[3], Heru Purwanto[4]
Fakultas Teknik Informatika, Jakarta Global University, Indonesia[1,2,3,4]
Email: edearniwati@gmail.com, gustinurlette@student.jgu.ac.id, saifulanwar@student.jgu.ac.id, h3ru.purwant0@gmail.com

ABSTRACT

Information Technology (IT) in the industrial world is an important part in the development of business processes and plays a vital role, including for PT Pamapersada Nusantara. To maintain the continuity of its business process activities, PT Pamapersada Nusantara is aware of the need for continuous control. This control effort is closely related to the increased risk from the application of information technology at PT Pamapersada Nusantara. Risks that have a negative impact have the potential to threaten the sustainability of the organization's business activities if they reach certain criteria, making it a disaster. This has prompted PT Pamapersada Nusantara to prepare for the possibility of a disaster. The purpose of this activity is to prepare an IT Disaster Recovery Plan (DRP) for PT Pamapersada Nusantara. DRP is a type of contingency plan that includes the preparation and response of an organization in the event of a disaster. The preparation of this DRP is guided by the NIST SP 800-34 framework, which begins with risk identification and assessment, Business Impact Analysis (BIA), identification of preventive controls and preparation of contingency strategies. After these steps have been taken, it is continued with the development of a contingency plan which includes plans for the activation phase, recovery phase and reconstitution phase. The result of this activity is a DRP document that is adapted to the organizational conditions of PT Pamapersada Nusantara. This DRP document contains a service recovery guide along with preventive measures before a disaster occurs. Keywords : disaster, risk, disaster recovery plan, NIST SP 800-34.

KEYWORDS *disaster, risk, disaster recovery plan, NIST SP 800-34*

How to cite: Erma Dearniwati, et al. (2025). Preparation of IT Disaster Recovery Plan (DRP) using NIST SP 800-34 Framework (Case Study: PT Pamapersada Nusantara, Jakarta). Journal Eduvest. *5*(1): 954-961s
E-ISSN: 2775-3727

INTRODUCTION

PT Pamapersada is a company engaged in coal mining. The company is centrally located in Pulogadung Industrial Estate, East Jakarta. PT Pamapersada itself has several job sites spread throughout Indonesia, including South Kalimantan, East Kalimantan, South Sumatra, and Warehouse Cileungsi. To maintain the continuity of its business activities, PT. Pamapersada realizes that there is a need for continuous control efforts. This control effort is closely related to the increasing risks that overshadow the application of information technology at PT. Pamapersada. Risks that have a negative impact, have the potential to threaten the continuity of the organization's business activities if they reach certain criteria that make it a disaster. Global facts show that many organizations that do not prepare for a disaster, have to pay dearly after experiencing a disaster, even some of them are forced to close due to losses. This is what PT Pamapersada avoids and encourages organizations to prepare for the possibility of a disaster (Alifian & Priharsari, 2021; Supriyanto et al., 2019).

Preparation for the possibility of a disaster can be done one of them by preparing a Disaster Recovery Plan (DRP). DRP is one type of contingency plan that includes preparation and response of the organization when a disaster occurs. The availability of DRP for an organization is a form of anticipation of possible delays in the provision of IT services due to damage and/or loss after a disaster. Any delay in the provision of IT services will affect the performance of the organization's business activities (Isa, 2020; Suhartono & Isnaini, 2021). In addition, DRP can also minimize the personal decision-making process during a disaster and encourage organizations to prepare for the possibility of a disaster. This is good, considering that the decision-making process carried out sporadically by certain parties will affect the length of time for decision-making and increase the potential for inconsistency of decisions taken.

Seeing the urgency and benefits of DRP in the organization, the Journal of IT Disaster Recovery Plan Design June 24, 2022 this activity was carried out in order to prepare a DRP for PT Pamapersada (M. Swanson, 2011; M. M. Swanson et al., 2002). DRP preparation can be done by applying existing frameworks, one of which is NIST SP 800-34, which is a standardization document issued by the National Institute of Standards and Technology (NIST) to provide instructions, recommendations, and considerations in preparing information system contingency plans.

Table 1. Information System Contingency Plans

Disaster	Causes
Natural	Disasters that occur due to natural processes, such as earthquakes, hurricanes, etc.
Human	Disasters that occur due to human negligence factors such as operator error, hijacking, virus spread, etc.

Environment	Disasters that occur due to environmental factors such as software system errors, telecommunications network damage, equipment errors, etc.

RESEARCH METHOD

Data Collection Stages

The stages of collecting data and material related to the focus of the problem to support the sharpness of the analysis of existing problems so as not to cause disasters to the company. This research directs the author to design a *Disaster Recovery Plan (DRP)* concept in the field of systems and information technology (*IT-DRP*) in coal mining companies to prevent disasters (Suhartono & Isnaini, 2021).

Writing Method

The writing method applied in this journal is a descriptive method with qualitative and quantitative approaches. Problem solving on the application of information technology using the *Disaster Recovery Plan (DRP)* concept is done by finding relevant literature (Prasetyo et al., 2019).

RESULT AND DISCUSSION

Risk Identification and Assessment

Companies that are able to manage risks well will be seen as having a sensitive ability to detect risks, have the flexibility to respond to risks and ensure resource capabilities to take action to reduce the level of risk, while those that cannot manage risks well will cause a waste of financial resources and time and not achieve company goals. Risk identification and assessment will provide an overview of the threats looming over the organization and the level of impact. The risk identification and assessment process in this study uses guidelines published by the company (Agung, 2019; Prabowo & Ramadhani, 2021).

Risk Identification

The identification process includes risks within the control and risks outside the control of PT Pamapersada Nusantara. This identification is carried out comprehensively on risk sources, causes, and controls that have been applied to these risks.

Table 2. The identification process

RISK THREAT CATEGORY	RISK THREATS	COMPONENTS DEVICE WHO ARE AT RISK

Nature	Earth movements (earthquakes, volcanic eruptions, etc.)	All IT Infrastructure Devices exposed
	Fire	
	Water (Flood)	
	Storm	
Services	Internet	Software (application software) and hardware (*hard disk*)
	Electricity	
	Gas	
	Air	
	Equipment failure	
Lost	Theft, breaking and entering, taking by force.	All IT Infrastructure Devices exposed
	Shootings, bombings	All IT Infrastructure Devices exposed
	Human Error	Software (application)
	Sabotage	Login access into the software
	Misuse of access rights for personal gain	Loss of critical data or loss of core business assets.
Device System Failure	- Functional failure - Code Error	Software

Risk Assessment

The identification results obtained findings in the form of 16 types of risks that envelop the existence of IT services at PT Pamapersada Nusantara. In addition to identifying risks, it is necessary to know the level of *likelihood*, and *impact of* the results obtained (Pratiwi, 2019; Santoso & Dirgantara, 2017; Yunita & Syafi'ah, 2021).

Risk Mapping of Policy Plan

The next stage in developing a contingency plan is to determine the contingency planning policy in the organization. The existence of this statement is

a form of commitment from senior management to participate in contingency planning. Matters related to the policy statement have been explained in the *NIST* 800-34 *framework*. The existence of this policy is needed as a guide so that contingency planning can run well and a form of senior management support in providing direction to the contingency planning program. The NIST 800-34 *framework* explains that policies in contingency planning contain at least the following:

- Purpose and scope of contingency
- Roles and responsibilities
- Training needs
- Training and testing scheduling
- Scheduling maintenance

Business Impact Analysis (BIA)

BIA is a stage to determine which services will be a priority for the Information Technology Department of PT Pamapersada Nusantara, especially in recovery. This stage will be carried out in three steps in accordance with the guidelines in *NIST SP* 800-34.

Service Criticality Assessment

This assessment is measured by determining the *estimated downtime* and measuring the *severity of impact* of each service owned by PT. Pamapersada Nusantara, where the determination of *estimated downtime* is a combination of *RPO, RTP* and *MTD*.

Service Complexity Level Assessment

This assessment is measured by assessing whether a service is complex or not based on agreed aspects, namely application system aspects and infrastructure aspects. The application system aspect has 3 assessment components, namely: installation, configuration, and testing. Meanwhile, the infrastructure aspect has 4 assessment components, namely: *security, backup, coverage,* and configuration.

Determining Recovery Priorities

Prioritization of service recovery is done by combining the results of criticality and service complexity assessments. The results of the combination of the two assessment components are then sorted from highest to lowest priority.

Identification of Preventive Controls

Preventive control analysis is carried out by identifying and assessing the 16 types of risks that have been collected, including current controls, control recommendations, and control types in accordance with the references followed.

Creation of Contingency Strategy

Backup Strategy

In order to maintain the continuity of system recovery activities, the backup process must be carried out regularly. Determination of *backup* frequency, *backup* type, and *backup* method is based on the needs and criticality of the data, in accordance with the guidelines that have been adopted. The proposed backup strategy is adjusted to the time required to tolerate data loss (*RPO*).

Alternative Locations

The selection of alternate sites is based on cost considerations and *RTO* assessment. Alternate sites can be managed in several ways, namely:

- Owned and operated by the organization itself
- Partnering with fellow subsidiaries of PT Pamapersada Nusantara
- Renting to a third party/vendor

Development of Contingency Plan

Supporting Information

In order for the contingency plan to work properly, the appointed team is expected to have clear roles and responsibilities. Each individual in the team is required to understand the objectives, roles and responsibilities assigned to them.

Some of the things that have been determined and established in the development of this contingency plan include:

- Roles and Responsibilities.
- Media Handling.
- Reserve Staff.
- *Assembly Point*
- *Data Center* Relocation.

Activation Phase

The activation phase is the initial stage carried out when an IT service disruption has been detected. This stage describes assessing system damage, notifying personnel, and activating the plan.

2 objectives that this stage is based on:

1. Assess the extent of the problem and the extent of the damage.
2. Determine whether further action is necessary.

Activities carried out at this stage:

- *Damage Assessment Team (DAT)* assesses the initial cause of the system disruption. This includes the type of disruption, location, and time of the disruption event.
- The *DAT* examines the damaged component and looks for the impact of the damage.
- *The DAT* checks the functional status of all components (e.g. fully functional, partially functional, or non-functional).
- *The DAT* checks for additional potential glitches or other system malfunctions.
- *DAT* checks for components that may need to be replaced (e.g. hardware, software, firmware, and supporting components).
- *DAT* classifies system disturbances.
- *The DAT* informs the *Contingency Plan Coordinator (CPC)* and the Recovery Team of the damage report.

Recovery Phase

This phase begins after contingency plans have been activated, notifications made, and the teams involved have been prepared. The recovery phase focuses on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or alternate location. Depending on the emergency event that occurs. Stages of activities performed by the *recovery team* include:

1. Identify recovery locations (location main or alternative location)
2. Prepare system documentation
3. Prepare resources that required to perform the procedure recovery includes backup media and personnel for recovery activation
4. Restore the system according to the system configuration
5. Perform device recovery that experiencing disruptions, including the operations, applications, and hardware (if needed)

Reconstruction Phase

The reconstruction phase is the last stage of the contingency plan implementation. During this phase, recovery activities have been completed and the system is operational again. This phase consists of two main activities, namely validating the recovery status, and terminating the plan.

Activities that should be done in this reconstitution phase include:

- Concurrent Processing;
- Data Validity Testing;
- Function Validity Testing;
- *Cleanup;*
- *Offsite Data Storage;*

- Data *Backup*
- Documentation;
- Deactivation of *DRP*.

CONCLUSION

PT Pamapersada is a company engaged in coal mining that has several job sites spread throughout Indonesia, including South Kalimantan, East Kalimantan, South Sumatra, and Warehouse Cileungsi. To maintain the continuity of its business activities, it is necessary to prepare for the possibility of a disaster, one of which can be done by preparing a Disaster Recovery Plan (DRP).

Disaster Recovery Plan is a solution for business continuity in response to disasters. With the replication of data and infrastructure, companies can easily continue to operate after a disaster. With *DRP*, in addition to minimizing financial losses, companies can also increase customer and investor confidence.

REFERENCES

Agung, M. Z. (2019). Perancangan disaster recovery plan sistem informasi akademik dengan pendekatan kerangka kerja nist 800-34. *JTERA (Jurnal Teknologi Rekayasa)*, *4*(2), 157.

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.

Isa, I. G. T. (2020). Implementasi Pendekatan Kerangka Kerja NIST 800-34 dalam Perancangan Disaster Recovery Plan pada Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi. *Jurnal Ilmiah Ilmu Komputer*, *15*.

Prabowo, W. A., & Ramadhani, R. D. (2021). Perancangan Contingency Planning Disaster Recovery Unit Teknologi Informasi Perguruan Tinggi menggunakan NIST SP800-34. *Techno. Com*, *20*(1).

Prasetyo, H. N., Supriatna, N., Raharjo, A. P., & Wikusna, W. (2019). Information technology disaster recovery plan (IT-DRP) model-based on NIST framework in Indonesia. *IJAIT (International Journal of Applied Information Technology)*, 34–45.

Pratiwi, R. A. (2019). *PERANCANGAN DISASTER RECOVERY PLAN PADA FASILITAS PUSAT DATA MENGGUNAKAN ISO 24762: 2008 (STUDI KASUS: FAKULTAS TEKNIK UNIVERSITAS PASUNDAN)*. Fakultas Teknik Unpas.

Santoso, G. B., & Dirgantara, D. (2017). Disaster Recovery Plan dalam Kantor Samisami. *PROSIDING SEMINAR NASIONAL CENDEKIAWAN*, 63–70.

Suhartono, D., & Isnaini, K. N. (2021). Strategi Recovery Plan Teknologi Informasi di Perguruan Tinggi Menggunakan Framework NIST SP 800-34. *MATRIK: Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *20*(2), 261–272.

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.

Swanson, M. (2011). *Contingency planning guide for federal information systems*. DIANE Publishing.

Swanson, M. M., Grance, T., & Hash, J. (2002). *Contingency planning guide for information technology systems*.

Yunita, I. R., & Syafi'ah, N. (2021). Pengembangan Disaster Recovery Plan Menghadapi Pandemi. *Jurnal Rekayasa Informasi*, *10*(1), 23–27.