JISS Journal of Indonesian Social Science

Vol. 4, No.09, September 2023
E-ISSN: 2723-6692
P-ISSN: 2723-6595
http://jiss.publikasiindonesia.id/

Disaster Recovery Plan Analysis Based on the NIST SP 800-34 Framework (Case Study: PT Wijaya Karya (Persero) Tbk.)

Eric Dwi Pamungkas[1], Nenden Siti Fatonah[2], Gerry Firmansyah[3], Habibullah Akbar[4]
[1,2,3,4] Universitas Esa Unggul, Indonesia
Email : ericdpamungkas@live.com, nenden.siti@esaunggul.ac.id, gerry@esaunggul.ac.id, habibullah.akbar@esaunggul.ac.id

KEYWORDS
Disaster Recovery Plan, BIA, NIST SP 800-34

ABSTRACT
PT Wijaya Karya (Persero) Tbk. (WIKA) is a state-owned company engaged in the construction sector and EPC is currently developing its business in the mining and investment sectors both at home and abroad. Information Technology is one of the supports to achieve its goals. The use of Information Technology is urgently needed by WIKA in order to increase the effectiveness and efficiency of the company's operational activities. In this regard, it is necessary to develop procedures for managing information technology resources to support WIKA's business continuity, which includes services for internal or external users. In the use of information technology, the Disaster Recovery Plan (DRP) is an important part of IT services in efforts to prevent Data Center Fail-Over caused by disasters. With the DRP procedure, it is expected that the Information Systems Bureau as the manager of WIKA's information technology can immediately anticipate if a Disturbance or Disaster occurs which has the potential to disrupt a large number (the majority) of processes or activities that are very critical for business continuity. This Disaster Recovery Plan is guided by the NIST SP 800-34 framework which begins with identifying and assessing risk, Business Impact Analysis (BIA), identification of preventive controls and preparation of contingency strategies.

1. Introduction

Talking about the country of Indonesia which is in the Pacific ring of fire region which is vulnerable to natural disasters. Actually, natural disasters have become a daily occurrence, but so far awareness of this has not been awakened. So risk management in natural disasters for companies is very necessary (Pereira, Wanderley, & Delgado, 2021).

Every company must have a risk management mechanism capable of dealing with these risks. Therefore, a Disaster Recovery Plan (DRP) is one of the requirements that must be owned by a company to reduce losses that may arise as a result of the disaster. With DRP, companies are expected to be able to provide sufficient security to safeguard the interests of a company's data.

Companies are also expected to reduce the risk of delays in providing data, especially during a disaster (Sydnor, Niehm, Lee, Marshall, & Schrank, 2017). Because, at this point the function and role of the company becomes very necessary. With the DRP, decisions will be taken quickly. Continuity of business services is one of the main prerequisites for service excellence. For IT-based services, the existence of a Disaster Recovery Plan is a core component of this sustainability capability.

2. Materials and Methods

The prelude to this chapter will delve into the Literature Review, a pivotal component in establishing the foundational knowledge and context for the researched topic.

Disaster

Disaster is an event or series of events that threatens and disrupts people's lives and livelihoods caused, both by natural factors and/or non-natural factors as well as human factors, resulting in human casualties, environmental damage, loss of property, and psychological impacts (BNPB 2023). In the current global economic scenario, organizations are more vulnerable to natural, human or technical problems. Every disaster, such as floods, fires and viruses and cyber terrorism, can affect the accessibility, honesty and privacy of key business resources. When categorized, disasters can be divided into two. Natural disasters are disasters caused by events or a series of events caused by nature include earthquakes, tsunamis, volcanic eruptions, floods, droughts, hurricanes, and landslides.

Non-natural disasters are disasters caused by events or a series of non-natural events which include technological failures, modernization failures, epidemics and disease outbreaks (Suhartono, Fatmawati, & Suranto, 2020). As for events that occur due to mistakes, stupidity, negligence from humans or even the evil intentions of individuals which result in losses to the surrounding environment. System failure, electricity, telecommunications, terrorism, cyber terrorism fall into this category.

Disaster Recovery Plan

Disaster Recovery Plan is a process/capability of an organization to respond to a disaster or interruption in services through the implementation of a disaster recovery plan to stabilize and restore the organization's critical functions (EC-Council 2017). This plan was created to help restore the company's business processes and reduce the impact if a disaster occurs which results in damage or loss of electronic data that supports the company's business processes (Omar, Alijani, & Mason, 2011; Sahebjamnia, Torabi, & Mansouri, 2015).

NIST SP 800-34

The NIST SP 800-34 framework is a standardization document issued by the National Institute of Standards and Technology (NIST) to provide guidance, recommendations and considerations in preparing information system contingency plans (Swanson et al. 2010). This framework identifies fundamental planning principles and practices to help personnel develop and maintain effective IT contingency plans. Principles meet most organizational needs, however it is recognized that each organization may have additional requirements

specific to its own processes (Alifian & Priharsari, 2021; Supriyanto, Aknuranda, & Putra, 2019). The document provides guidance to help personnel evaluate information systems and operations to determine contingency needs and priorities. This guide also provides a structured approach to assist planners in developing cost-effective solutions that accurately reflect their IT needs and integrates contingency planning principles into all aspects of IT operations. The guidance presented should be considered during each stage of contingency planning, starting with the conceptualization of the contingency planning effort through the maintenance of the plan and the deletion of the contingency plan. When used as a planning management tool during the contingency planning process, this document and its annexes should provide users with time and cost saving practices.

Literature Review

Literature Study is a method that identifies, assesses, and interprets findings on a research topic to answer predetermined research questions (Paré & Kitsiou, 2017). This SLR study follows the stages of planning, conducting, reporting. The research stage which consists of the planning stage which is the initial stage of conducting SLRs, then entering the conducting stage, namely the implementation stage of the SLRs, and the final stage, namely reporting, which is the stage of writing SLRs into a report.

Research Methodology

This research is based on the NIST SP 800-34 framework. Where this framework is one of many documents originating from the National Institute of Standards and Technology (NIST). This framework contains recommendations, instructions, and considerations when developing contingency plans (Barker & Barker, 2018). The focus of preparing a contingency plan on NIST SP 800-34 is in the form of early stages in handling after a disaster. Temporary treatment such as relocating services and their operations to an alternative location, or doing it manually is also a contingency plan. This framework contains a contingency plan development phase which includes 7 stages(Swanson et al. 2010).

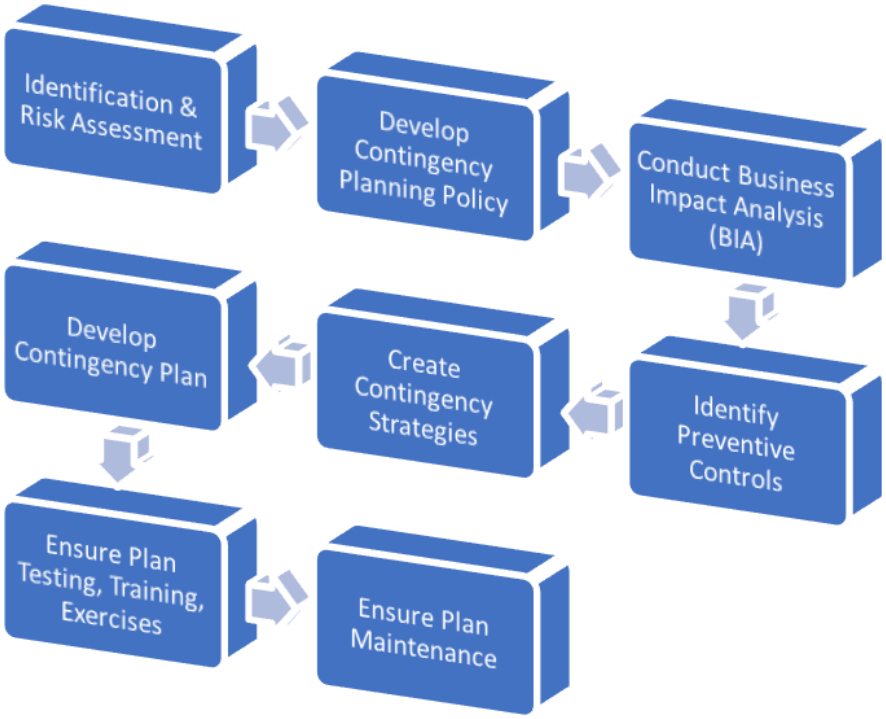

Figure 1. Research Methodology

3. Results and Discussions

In this chapter, the author will conduct an analysis of the Disaster Recovery Plan based on the NIST SP 800-34 framework. Covers all the stages in this framework.

Identification and Risk Assessment

The stages of risk identification and assessment are carried out on IT assets and services within the scope of WIKA. Where data collection was carried out using interviews and questionnaires for the stages of identification and risk assessment. The personnel who will be used as sources are the PICs of each IT service holder.

The risk identification stage produces output in the form of a list of risks that impact IT assets and services. Where the risk list contains sources of risk, causes, and controls that have been carried out. The risk assessment stage is carried out after obtaining a list of risks that impact IT assets and services. The list of risks was then assessed using a questionnaire method which was submitted to informants based on predetermined risk assessment criteria, namely likelihood criteria and consequence criteria.

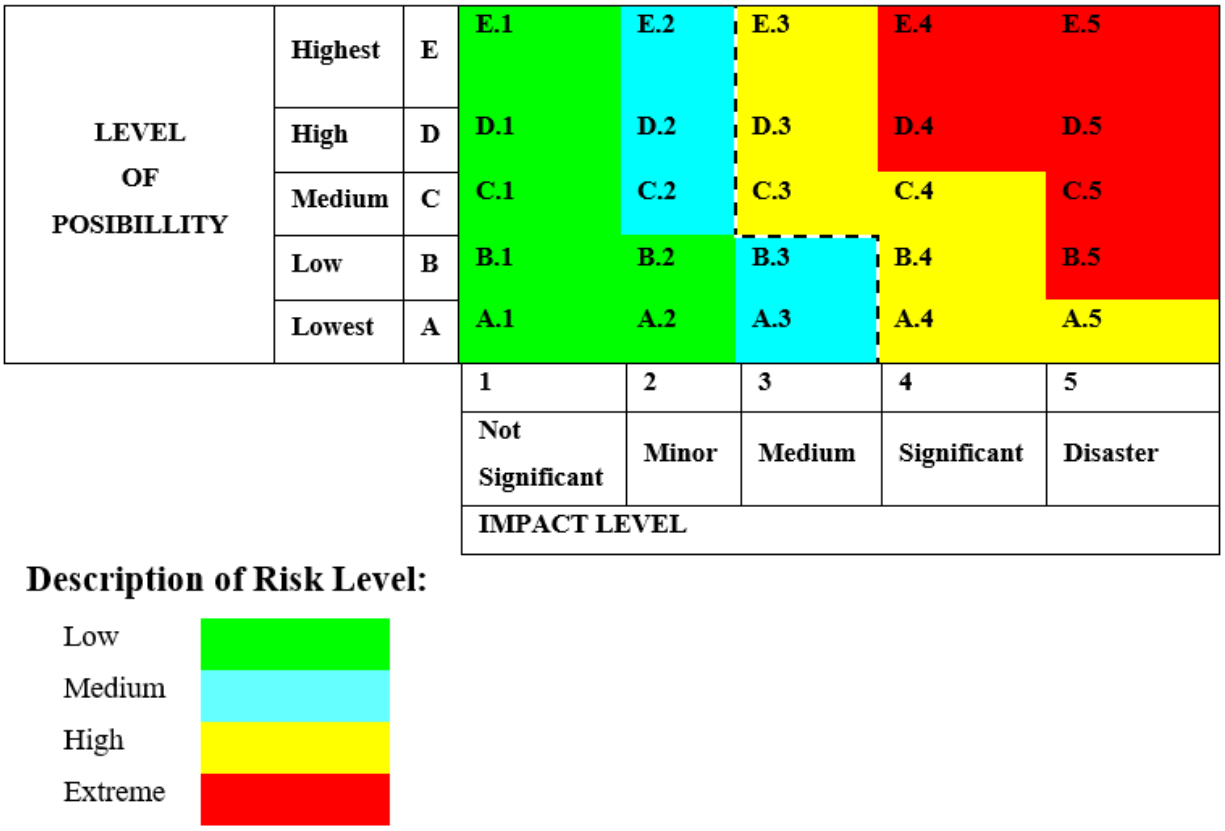

Figure 2. *Risk Matrix*

The Risk Matrix will show a risk map, which divides risk into four categories, namely Low (cells in green), Moderate (cells in blue), high (cells in yellow), and extreme (cells in red). The risk appetite tolerated by the company is low and moderate risk.

Contingency Policy Plan

The contingency policy plan aims to determine the contingency planning policy within the organization. This plan is a form of commitment from management to contribute to contingency planning. Related matters in 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. In addition, the existence of this policy is also a form of management support to provide direction for the contingency planning program.

This plan demonstrates that to be effective and to ensure that staff fully understand the organization's contingency planning requirements, the contingency plan must be based on a clear policy. The contingency planning policy statement should define the organization's overall contingency objectives and define the organization's framework and responsibilities for system contingency planning. To be successful, top management must support the emergency program and be included in the program's policy development process.

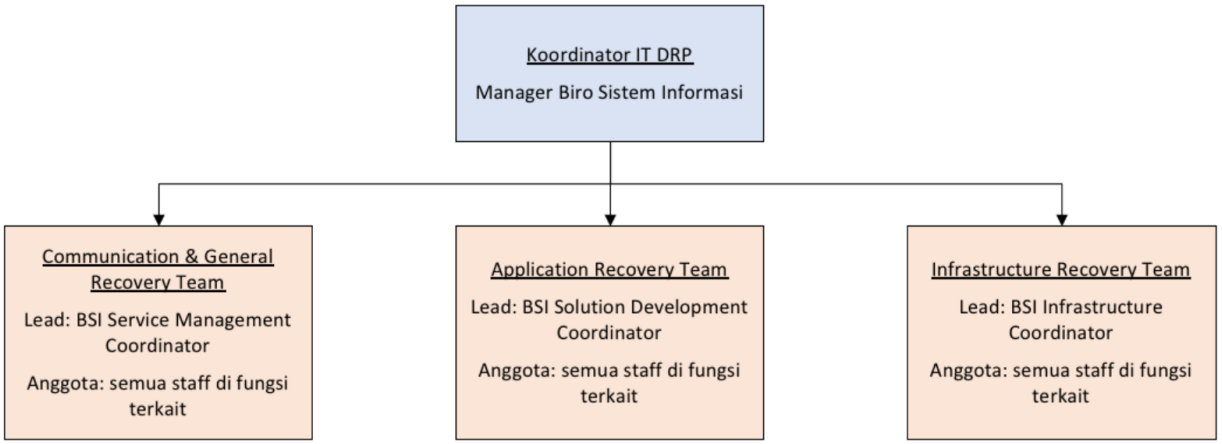

Figure 3. *DRP IT Team*

The DRP IT Team is the core personnel of the DRP working under the supervision of the Bureau Manager. This team is tasked with implementing DRP when a disaster occurs within the company, and ensuring that DRP is implemented thoroughly. Each member of the DRP IT Team is given training in accordance with their functions and duties. The purpose of the training is to ensure that each member understands their respective duties and has the ability to perform their corrective function. This must be done once every 1 (one) year if the system/network configuration changes or a new system is added to the existing IT DRP system.

After the team is formed and a team training plan is made, the need for a maintenance plan is an action taken to maintain and improve a service until it becomes an acceptable condition. This plan must be updated regularly in order to adapt to developments/changes in the organization.

Business Impact Analysis (BIA)

BIA is the process of analyzing business functions and the impact of business interruptions on them (Păunescu, Popescu, & Blid, 2018). BIA can also perform management-level analysis that organizations use to assess the quantitative and qualitative impacts, effects, and losses that could occur in the event of an emergency, incident, or crisis. BIA findings are used to make decisions about Business Continuity strategies and solutions (Hassel & Cedergren, 2021). BIA helps identify what will be lost if business is disrupted, which can lead to lost profits and revenue, deteriorating customer relationships, loss of reputation. It is also a key process for understanding how much disruption each process or task can tolerate before the damage is irreparable and on which resources (people, machines, documents, or other processes) the company depends on.

Identification of Preventive Controls

In some cases, the service interruption impacts identified in the BIA can be mitigated or eliminated through preventive measures that deter, detect and/or reduce the impacts on the system. Where feasible and cost-effective, preventative methods are preferred over actions that may be necessary to recover the system after an outage. The second step includes

identifying effective preventive controls for contingency planning and maintaining these controls on an ongoing basis. This stage is also to determine the response from the list of risks that have been identified in the previous stage. As well as this is useful as a mitigation measure and the impact of risks that will endanger the services of the organization.

Contingency Strategy Development

This Contingency Strategy includes a backup strategy and determining alternative locations. Several services will be determined by their backup strategy including method and frequency. Backups on IT services need to be done regularly. The following table contains recommendations regarding the backup strategy to be carried out. This backup strategy is based on the priority level of IT services. For high priority, it requires a continuous backup using the Mirroring method in addition to using the Tape Backup method on a daily basis.

Table 1. List of Recommended Backup Strategies

No	Application Name	Backup Method	Backup Frequency	Backup Type
1	Human Capital Information System	Mirroring	Continuously	Full
2	WIKA PIS	Mirroring	Continuously	Full
3	CRM	Mirroring	Continuously	Full
4	SCM	Mirroring	Continuously	Full
5	Wika Zone (WZONE)	Mirroring	Continuously	Full
6	Administrasi Surat	Mirroring	Continuously	Full
7	Knowledge Management	Mirroring	Continuously	Full
8	SIMDIV	Mirroring	Continuously	Full
9	Nasabah Online	Mirroring	Continuously	Full
10	Fastbank Online	Mirroring	Continuously	Full
11	Dashboard BI	Mirroring	Continuously	Full
12	FMS	Mirroring	Continuously	Full
13	PMCS	Mirroring	Continuously	Full
14	QHSE	Mirroring	Continuously	Full
15	E-Meeting	Tape Backup	Daily	Incremental

Contingency Plan Development

The development of this plan includes 3 phases, namely activation, recovery and reconstitution. This plan was designed based on company conditions and involved several personnel. The involvement of several personnel in the context of data collection is in the form of a decision that must be given to complete the contingency plan that will be made. The Activation Phase occurs when IT services are detected to be problematic or experiencing disruptions. This phase will define how problems or disturbances are detected and categorized as a disaster and require DRP activation.

The recovery phase runs when DRP is activated and has been informed to all components of the company. In this phase, repairs to services or data center facilities are carried out immediately. If it is not possible to return to the original place, prepared an alternative area.

The Reconstitution Phase where the recovery process has been completed, this is also like the system recovery procedure, inspections must also be carried out every time there is a major change to the IT system and/or after testing. It is also necessary to periodically check to ensure that the latest patch/version/configuration information for this system is up to date.

Testing, Training, and Practice Plans

This stage helps the organization determine the effectiveness of the plan and helps all staff know their role in directing each information system plan. The test plan makes it possible to identify and address deficiencies in the plan by validating one or more system components and the operation of the plan. Testing can take many forms and serve a variety of purposes, but should be carried out as closely as possible to the operational environment. To be able to respond to an emergency situation, a Disaster Recovery Strategy Representation Diagram is prepared as follows.

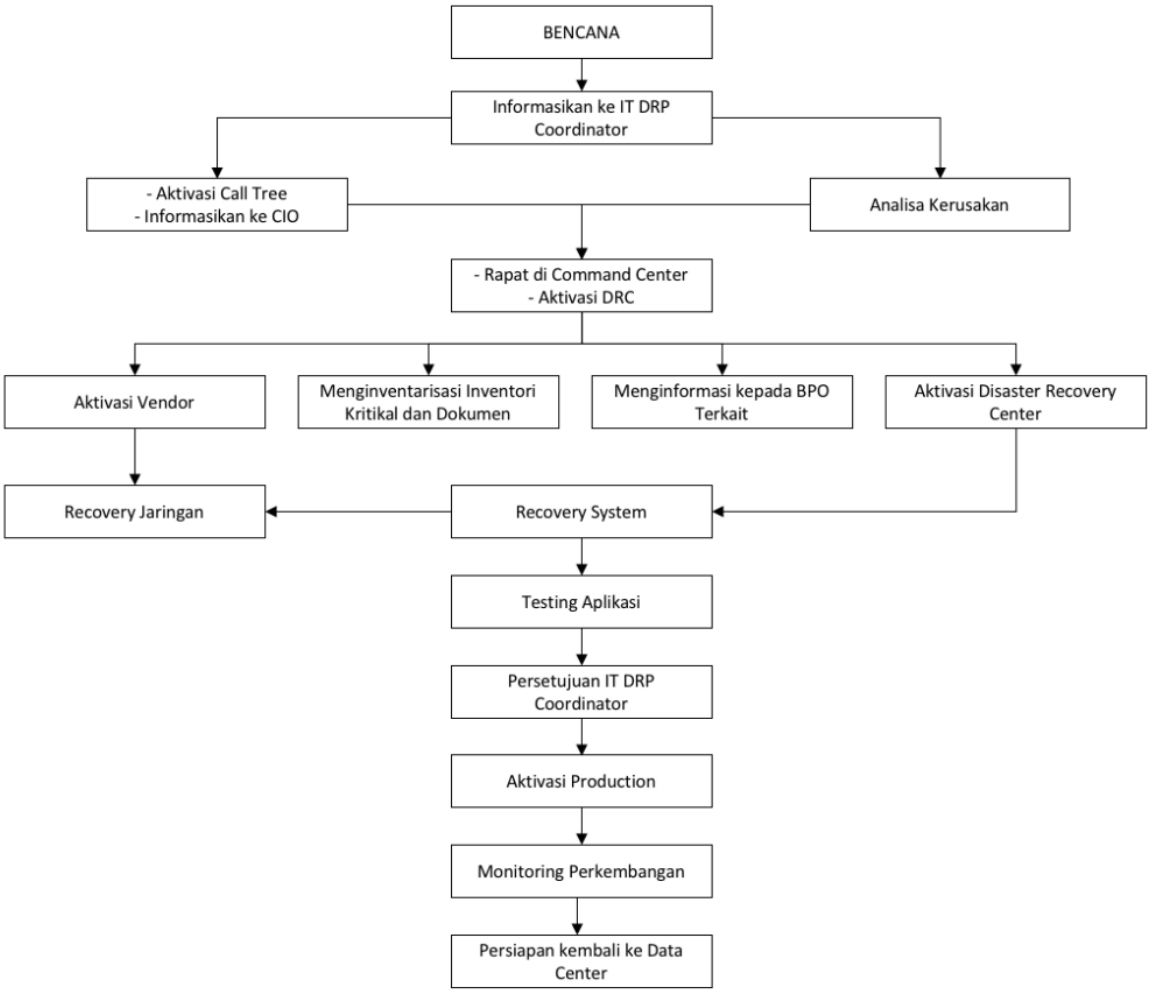

Figure 4. *Strategy Representation Chart*

Additionally training for personnel with contingency planning responsibilities should focus on familiarizing themselves with the roles and skills required to fulfill those responsibilities. This approach helps ensure that personnel are ready to participate in testing and training, as well as actual fault events. Training must be given at least once a year. Personnel should be trained to the extent that they can carry out activities appropriate to their roles and responsibilities without the aid of documentation.

There is a pilot training scenario with the following cases, On August 8, 2023, at 23.00 WIB there was a fire in the WIKA TOWER Building. The fire point is in the commissioner's room which is on the 5th floor and is also on the same floor as the Data Center. The fire was seen by security officers who were on duty that night. Assuming that the electricity is cut off to the 5th floor and some of the data center equipment is physically damaged so that some system functions are disrupted. Then at 23.45 the East Jakarta area fire team arrived at the location to immediately carry out the extinguishing process. After that, on August 9, 2023, at 00.45 WIT, all fires were successfully extinguished, assuming that some of the equipment experienced physical damage, so that the system that is still running is only 70% of maximum

capacity and PLN's electricity supply has not recovered and most likely will not recover in a short time.

Maintenance Plans

As part of the recovery plan policy, the DRP needs to be kept up to date, as during the operations phase there are frequent changes in the organization and therefore all changes must be tracked and reported to the process area. Changes in the organization that must be considered at the human resources level, implementation of new processes, acquisition and manufacture of new products, security requirements, among others. An important part of keeping the plan up to date is reviewing the overall plan at least once a year with all stakeholders.

To ensure the effectiveness and accuracy of IT DRP, each team coordinator must ensure that maintenance and updates have been carried out periodically and that data accuracy has been tested from both the DRP TEAM and BSI as well as WIKA IT service users. The following is a list of maintenance actions that must be carried out periodically.

No	Tindakan Pemeliharaan	Frekuensi	Penanggung Jawab
1	Pemeriksaan Tim dan Informasi Kontak	1 tahun	IT DRP Coordinator
2	Pelatihan Tim DRP	1 tahun	IT DRP Coordinator
3	Pengujian	1 tahun	IT DRP Coordinator
4	Pemeriksaan Perjanjian Vendor	Tahunan atau setelah ada perubahan besar terhadap	Application Recovery & Infrastructure Recovery Coordinator
5	Pemeriksaan Strategi Recovery	Tahunan atau setelah ada perubahan besar terhadap sistem atau perusahaan	Seluruh TimRecovery
6	Pemeriksaan Konfigurasi & Prosedur Recovery Sistem	Tahunan atau setelah ada perubahan besar terhadap sistem atau perusahaan	Seluruh TimRecovery

Figure 5. *Strategy Representation Chart*

4. Conclusion

A Disaster Recovery Plan is a stage of activities aimed at reducing the likelihood and limiting disaster losses in critical business processes. With DRP as a guideline for dealing with disasters, companies can deal with critical situations due to disasters in a better and more focused manner.

In this DRP there are various risks originating from Nature, Humans, and the Building Environment. There are also IT services with varying degrees of criticality. Based on the results, there are 5 applications that are categorized as applications with a high priority level, namely HCIS, WIKA PIS, CRM, SCM, and WZONE. There are 9 applications with medium priority level, namely Administrasi Surat, Knowledge Management, SIMDIV, Nasabah Online, Fastbank Online, BI Dashboard, FMS, PMCS, and QHSE. While applications with a low level of criticality there is 1 application, namely E-Meeting. This IT service has been tested based on

threats that will occur, one of which is the scenario where the Data Center experiences a power failure caused by a fire.

This DRP has 3 phases namely the Activation Phase, the Recovery Phase, and the Reconstitution Phase. The Activation Phase occurs when IT services are detected to be problematic or experiencing disruptions. This stage will define how problems or disturbances are detected and categorized as a disaster and demand DRP activation. This recovery phase runs when DRP is activated and has been informed to all components of the company. At this stage, repairs to services or data center facilities are carried out immediately. The Reconstitution Stage where the recovery process has been completed, this is also like a system recovery procedure, an inspection must also be carried out every time there is a major change to the IT system and/or after testing. It is also necessary to periodically check to ensure that the latest patch/version/configuration information for this system is up to date.

5. References

Alifian, Muhammad Hilal, & Priharsari, Diah. (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.

Barker, Elaine, & Barker, William. (2018). *Recommendation for key management, part 2: best practices for key management organization*. National Institute of Standards and Technology.

Hassel, Henrik, & Cedergren, Alexander. (2021). Integrating risk assessment and business impact assessment in the public crisis management sector. *International Journal of Disaster Risk Reduction*, *56*, 102136.

Omar, Adnan, Alijani, David, & Mason, Roosevelt. (2011). Information technology disaster recovery plan: Case study. *Academy of Strategic Management Journal*, *10*(2), 127.

Paré, Guy, & Kitsiou, Spyros. (2017). Methods for literature reviews. In *Handbook of eHealth evaluation: An evidence-based approach [Internet]*. University of Victoria.

Păunescu, Carmen, Popescu, Mihaela Cornelia, & Blid, Laura. (2018). Business impact analysis for business continuity: Evidence from Romanian enterprises on critical functions. *Management & Marketing. Challenges for the Knowledge Society*, *13*(3), 1035–1050.

Pereira, Renato Marques Sanches, Wanderley, Henderson Silva, & Delgado, Rafael Coll. (2021). Homogeneous regions for rainfall distribution in the city of Rio de Janeiro associated with the risk of natural disasters. *Natural Hazards*, 1–19.

Sahebjamnia, Navid, Torabi, S. Ali, & Mansouri, S. Afshin. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal of Operational Research*, *242*(1), 261–273.

Suhartono, Fatmawati, Sri, & Suranto. (2020). Non-Natural Disaster Mitigation Covid-19 Pandemic and its Urgency in the Education Curriculum. *Proceedings of the 4th International Conference on Learning Innovation and Quality Education*, 1–5.

Supriyanto, Adi, Aknuranda, Ismiarta, & Putra, Widhy Hayuhardhika Nugraha. (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.

Sydnor, Sandra, Niehm, Linda, Lee, Yoon, Marshall, Maria, & Schrank, Holly. (2017). Analysis of post-disaster damage and disruptive impacts on the operating status of small businesses after Hurricane Katrina. *Natural Hazards*, *85*, 1637–1663.

BNPB. 2023. "Definisi Bencana - BNPB." *Https://Bnpb.Go.Id/Definisi-Bencana*. Retrieved July 15, 2023 (https://bnpb.go.id/definisi-bencana).

EC-Council. 2017. *Disaster Recovery and Business Continuity*.

Swanson, M., P. Bowen, A. W. Phillips, D. Gallup, and D. Lynes. 2010. *Contingency Planning Guide for Federal Information Systems*. Gaithersburg, MD. doi: 10.6028/NIST.SP.800-34r1.