International Journal
of Applied Information Technology

http://journals.telkomuniversity.ac.id/ijait/

Information Technology Disaster Recovery Plan (IT-DRP) Model-Based on NIST Framework in Indonesia

Hanung Nindito Prasetyo [a,*], Nana Supriatna [b], Anugrah Pambudi Raharjo [c] Wawa Wikusna [d]

[a,d] *Diploma of Information System, School of Applied Science, Telkom University, Indonesia*
[b] *Daya Sinergi Teknomandiri, Indonesia*
[c] *Dept. of IT Management, Ministry of Women's Empowerment and Child Protection of The Republic of Indonesia*

hanungnp@tass.telkomuniversity.ac.id, supriatna.nana.gm@gmail.com, anugrah@kemenpppa.go.id, wawa_wikusna@tass.telkomuniversity.ac.id

ARTICLE INFO

Received 8 November 2019
Revised 19 December 2019
Accepted 27 December 2019
Available online 15 Januari 2020

Keywords
Information Technology, Disaster Recovery Plan, NIST Framework

ABSTRACT

Based on data, Indonesia ranks second in the list of the highest number of deaths due to natural disasters in the Asia-Pacific. Over the past 20 years, various natural disasters in this country have also caused economic losses of at least US$ 22.5 billion. This data means that disasters in various sizes and scales can occur and affect business. Disaster threats can occur in various forms, such as earthquakes, tsunamis, and floods. The threat of disasters will certainly disrupt and can have a fatal impact on the sustainability of business supported by information technology, the Ministry of Women's Empowerment and Child Protection (KPPPA) as a case study has an interest in this matter. One of the infrastructures that become an essential asset as the performance support capacity of the KPPPA is an information system and technology. System tools and Information technology are business process support tools at the KPPPA so that businesses have sustainability and can run well. Disasters that occur will undoubtedly have a fundamental impact that can damage the system and technology in the organization so that it will positively affect the course of business processes. For this reason, integrated planning is needed to handle the disaster so that business processes can continue to run as they should. One of the integrated plans is designing an Information Technology and Communication Disaster Recovery Plan (IT-DRP). This study discusses the NIST framework implementation as one of the IT-DRP models which have been applied in KPPPA.

* Corresponding author at:
School of Applied Science, Telkom University
Bandung Technoplex, Telekomunikasi Street, Terusan Buah Batu, Bandung, West Java 40257
Indonesia
E-mail address: hanungnp@tass.telkomuniversity.ac.id

ORCID ID:
First Author: 0000-0001-5717-9337

https://doi.org/10.25124/ijait.v3i01.2317

1. Introduction

The Asian region is at the top of the list of victims due to natural disasters. Nearly half of the world's disasters occur in Asia, making this region prone to disasters. The report from ESCAP also detailed a list of countries in the Asia Pacific region experiencing natural disasters during the period 1980-2009. For example, Indonesia ranks second in the list of the highest number of deaths due to natural disasters in the Asia-Pacific. Over the past 20 years, various natural disasters in this country have also caused economic losses of at least US $ 22, 5 billion [1]. This data means that disasters in various sizes and scales can occur and affect business. Disaster threats can occur in various forms, such as earthquakes, tsunamis, and floods. One potential earthquake disaster, as found by Australian geodetic researcher Achraff Koulali, in 2016, published his findings of active faults crossing about 25 kilometers south of Jakarta, stands for the Baribis Fault. Where the earthquake from this fault can potentially reach 7 (seven) on the Richter scale, and this is confirmed by simulations of Nguyen researchers from GeoScienc Australia [2] [3]. Another potential threat is the potential for a tsunami to occur either due to an earthquake or not, as the results of a BPPT study in the form of a potential tsunami simulation research results from DR. Widjo Kongko carried out in western Java including Jakarta and Banten. The results of the study show that the southern part of Java island has a high tsunami potential, including the Jakarta area, where the simulation shows the potential of the tsunami height average to reach 12 meters [4].

In this study, the Ministry of Women's Empowerment and Child Protection (KPPPA), as a case study, certainly has an interest in this matter. One of the infrastructures that become an essential asset as the performance support capacity of the KPPPA is a system of information systems and technology. System tools and Information technology are business process support tools at the KPPPA so that businesses have sustainability and can run well. Disasters that occur will undoubtedly have a fundamental impact that can damage the system and technology in the organization so that it will positively affect the course of business processes. It is on this basis that disaster management is needed from the start of preparedness, events, and disaster recovery, especially in the field of information systems and technology within the KPPPA.

As one of the results of the recommendations from the results of the BMKG scientific study regarding this matter is now ready to face the potential for disasters, both earthquakes, tsunamis, floods, and others, what should be done and not wait when [5]. Based on this awareness, the KPPPA needs to realize readiness regarding potential disasters that can occur at any time. The types of disasters are as follows.

1. Level 1, Computer Failure, Corrupted, Data, Labor Issues, Lost Data, Medical Emergencies, Network Failure, Software Errors.
2. Level 2, Bomb Threat, Bomb Blast, Biological Attack, Chemical, Spill / Attack, Civil Unrest, Computer Virus, EMP, Espionage, Hacking, Human Error, Legal Issues, Logic Bomb, Sabotage, Theft, Terrorism, Workplace Violence.
3. Level 3, Blackouts, Brownouts, Burst Pipe, Environmental Hazards, Epidemics, Evacuation, Halon Discharge, HVAC Failure, WAN / ISP Failure, Power Surge, Failure Power Grid, Sprinkler System Discharge, Transportation Disruptions.
4. Level 4, Earthquakes, Electrical Storms, Fire, Flooding, Hurricanes, Lightning, Tornadoes, Tsunamis, Volcano, Wind, and Winter storms.

For this reason, integrated planning is needed to handle the disaster so that business processes can continue to run as they should. One of the centralized planning is designing an integrated Information Technology and Communication Disaster recovery plan (IT-DRP) [10]. IT-DRP document contains the work guidelines that are ready to be executed at the time before they occur. Also, after a condition outside the regular (accident, disaster, etc.) occur to ascertain the activities of the Service and Information Technology process. Mainly related to Applications and supporting infrastructure within the Ministry of Women's Empowerment and Child Protection or the KPPPA can run smoothly. The effort that must be made is related to the readiness of personnel and service processing facilities in the face of disasters that occur due to nature or human activities. Also, the existence of disaster recovery planning documents, especially in the field of systems and information technology, is an essential requirement in Information technology governance in organizations, which of course, in this case, is the KPPPA.

The Ministry of PPPA requires a draft comprehensive IT-DRP document to be implemented in an emergency related to System and Information Technology operations. Therefore, the appearance of regular outbreaks can be minimized, and IT Services can be restored according to the Maximum Tolerable Period requirements of Disruption (MTPD), which has been defined according to standards Risk Assessment (Risk Assessment).

2. Literature Review

2.1 Information Technology Disaster Recovery Plan (IT-DRP)

Disaster Recovery Plan (DRP) in the field of system and information technology or can be abbreviated as IT-DRP is a written and approved the program, implemented, and periodically evaluated, which focuses on all activities that need to be done before, during, and after a disaster. This plan is prepared based on a thorough review of potential disasters, which cover the scope of facilities, geographical location, or industry. This plan is also a statement of the right response to the recovery process that is effective against cost, time, and speed [6].

IT-DRP must also include procedures to respond to an emergency, provide operational backups as long as the disturbance occurs, and manage recovery and save the process afterward. The main objective of a disaster recovery plan is to provide the ability to apply critical processes in other locations. Then, return them to their original locations and conditions within a time limit that minimizes losses to organizations. Notably, in this case, the Ministry of Women's Empowerment and Child Protection, with rapid recovery procedures and measurable.

2.2 NIST SP 800-34 Framework

National Institute for Standards and Technology (NIST) Special Publication (SP) 800-34 is a guide that contains instructions, recommendations, and decisions in making plans for information system recovery after a disaster or disruption occurs. NIST SP 800-34 was published in 2010 in May. In NIST SP 800-34, the disaster recovery process is divided into three parts, namely [7]:

1. Activation and Notification. This stage is the stage of decision making when a disaster occurs and notifies the incident to the recovery team members to implement IT-DRP. At the end of this stage, the recovery team must be ready to carry out the planned recovery process

2. Recovery. This part is the stage of restoring system services and information technology as a whole so that the business process can run again. At the end of this stage, the information system and technology has been running smoothly.
3. Reconstruction. This stage is the stage where when all systems have been successfully restarted even though temporarily. Moreover, in this stage, all operational activities are returned to their initial conditions before the disaster occurs. If the initial facility cannot be restored, then prepare new facilities and places according to the activities planned at this stage.

The implementation of the system and technology disaster recovery plan. The information compiled is based on the National Institute for Standards and Technology (NIST) standards, a special publication with number 800-34, concerning Contingency Planning for Information Technology Systems.

3. Research Methods

3.1 Types of Research

This type of research is exploratory research with a qualitative descriptive research design. The purpose of this study was to introduce the concept of IT Disaster Recovery to be more easily implemented in a variety of organizations, provides a basic overview of the IT Disaster Recovery Plan, opportunities are likely to be holding further research on this study.

3.2 Object of Research

The object of this research is the design of the IT disaster recovery plan at the KPPPA Republic of Indonesia Ministry, which is linked to the vision, the mission of the organization to be a business process, and strategy to achieve a competitive advantage.

3.3 Research Steps

In this study, the steps taken are as follows.

1. The analysis system is running. In this step, an analysis of the system is running on KPPPA.
2. Determine the formulation of the running system problem. In this step, grouping information from the analysis of the results can carry out at the stage of analysis of the system is running.
3. Study of literature. In this step, a literature study is conducted to find a solution to the problem. The results obtained in this step obtain methods and frameworks to solve existing problems, namely using the NIST SP 800-34 framework
4. IT-DRP Designing. At step above a predetermined method to settle the problem in this study, it is at this step in doing the design by doing the mapping information on the framework used

4. Design of KPPPA RI Disaster Recovery Plan

4.1 Modeling

The modeling carried out is based on 7 (seven) principles in the NIST SP 800-34 framework, namely [7]:

1. There is a contingency planning policy statement formally made by the organization as the authority and guidance needed to develop an effective contingency plan.
2. Conduct a business impact analysis. The business impact analysis helps identify and prioritize critical Information Technology systems and components.
3. Identification of preventive controls. These are steps taken to reduce the effects of system interruptions and can increase system availability and reduce contingency life cycle costs.
4. Determine recovery strategies. A comprehensive recovery strategy that ensures that the system can recover quickly and effectively after a disaster or disruption.
5. Determine the Information Technology contingency plan. Contingency plans must contain detailed guidelines and procedures for recovering systems damaged by disasters or disturbances.
6. Develop and implement planning testing, training, and training. Hold training to prepare recovery personnel to activate plans to improve the effectiveness and readiness of the overall disaster recovery team.
7. Planning treatment. The plan must be a periodically updated document in accordance with the improvement of information systems and technology within the organization.

4.2 Policy Statement

The determination of policy realization is a direct reflection of the commitment of KPPPA. They implement the IT Service Continuity Plan and IT Disaster Recovery Plan at the ministry's internal level to comply with and follow best practices according to national and international standards. The policy statement is clearly stated in the organization's strategy document [11].

4.3 Analysis of Business Impact.

In accordance with accepted international best practices, IT DRP will determine the mechanism for recovery from disaster damage such as strategic importance, total technological damage, loss of core IT staff, or various matters related to the above. Continuity of IT Services will be carried out with due regard to definitions and agreements that such catastrophic events can cause severe damage that can lead to business continuity and loss of life. The business impact analysis on KPPPA RI is done as an effort to find out the priority scale in handling disasters. One way that can be done is to determine the main process of IT services at KPPPA, namely:

1. Internet Access Service
2. IT Server Service
3. Application management services
4. Presence System Services

4.4 Prevention Control Analysis

Based on the business impact analysis, the four services are the focus of process risk analysis. By using risk analysis by presenting the analysis using the following Figure 1.

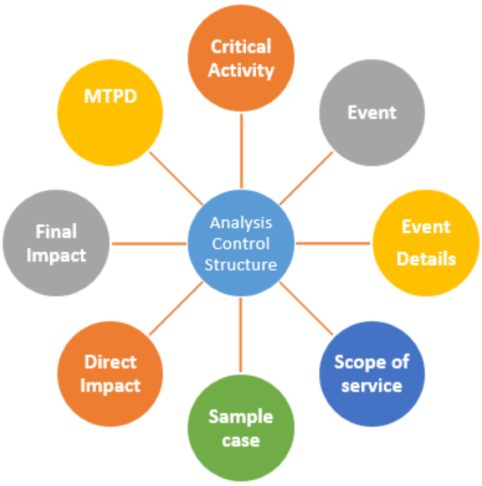

Figure 1 Control Analysis Model

Based on risk analysis, the main services obtained are the priority scale, namely:

1. Internet access service, including
   - Internet access
   - Electric Supply
2. Server Service, including
   - Security
   - Storage
   - Electric Supply

The two service items are a priority in handling IT-DRP within the KPPPA compared to attendance system services and application management services for the systems and information technology fields.

4.5 Determination of Recovery Strategy

Information is an essential part of the company's operations. Along with the increasing dependence of business on information technology, it also increases the risk of disasters due to business continuity. To deal with disasters that cannot be predicted, then the strategic approach related to system recovery and technology, the KPPPA uses the Hotsite strategy. The Hotsite strategy is carried out by building and collaborating with third parties regarding facilities backup system that is fully configured and ready to operate in a short time. The system must be compatible with backup data from the leading site and does not cause interoperability problems. This strategy can support the short /long term and is flexible in terms of configuration and choice. Thus, the company needs to have backup data storage that is used when an emergency. The backup data center must be far from the main location of the company to avoid events that coincide in the central location. Also, the backup data center must be able to be accessed at any time if the company needs it.

4.6 Determination of Information Technology Contingency Plans.

4.6.1 Recovery Flow

Figure 2 shows the recovery flow.

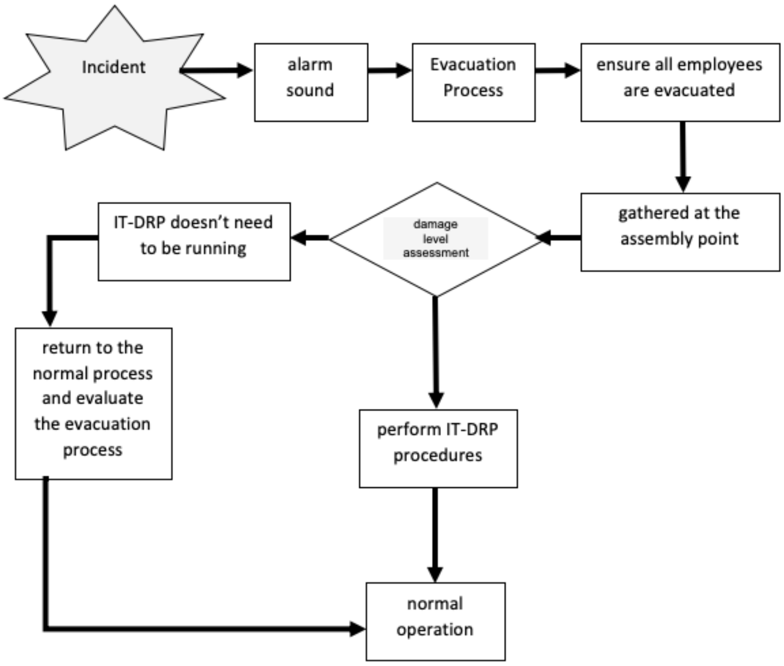
Incident
alarm sound
Evacuation Process
ensure all employees are evacuated
gathered at the assembly point
damage level assessment
IT-DRP doesn't need to be running
return to the normal process and evaluate the evacuation process
perform IT-DRP procedures
normal operation

Figure 2 IT-Recovery Process of KPPPA

4.6.2 Determining the Point Gathering (Assembly Point)

When there is a disaster, companies need to evacuate employees and customers by collecting them at a rallying point to facilitate the evacuation process. The gathering point must have a safe distance from the building or location hit by the disaster. The gathering point in the Ministry of Women's Empowerment and Child Protection is at:

1. Main location: Next to the KPPPA yard building
2. Backup location: Back Gate of KPPPA Building

4.6.3 IT-DRP Team (IT Disaster Recovery Team)

During an emergency, an IT Disaster Recovery Team or IT-DRP Team is the party that implements IT-DRP procedures as an effort to overcome the emergency. The IT-DRP Team of the Ministry of Women's Empowerment and Child Protection has the following assignments.

1. Contact emergencies from the local environment (fire, police, ambulance, etc.)
2. Establish an emergency relief facility with the help of local security and medical staff within 2 hours.
3. Conduct disaster impact assessments that are related to System and Information Technology infrastructure.
4. Restore the overall services of the company, especially in the field of systems and technology within 1 X 24 hours.

The structure of the IT-DRP team is in accordance with the needs of the KPPPA as follows (Figure 3).

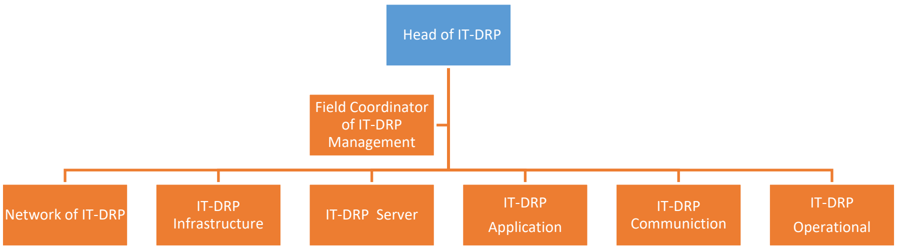

Figure 3 Team Structure of IT-DRP

4.6.4 Data Center Relocation as an IT-DRP Data Recovery Center

The backup data center must be far from the central location of the company to avoid events that coincide in the central location. Also, the backup data center must be able to be accessed at any time if the company needs it. KPPPA determines the relocation of the Data Center by referring to the rules of BAPPEPPAM & LK. It regulates disaster recovery and refers to ISO 27001, which is located at least 30 km to minimize disasters in the same area and in accordance with the provisions that hot site placement must minimize risk, meaning not p there is a fault line [8][9].

4.6.5 Media Handling

In an emergency, the company needs to coordinate with the media as agreed with the company's directors to avoid adverse publications in the community, especially related to system services and infrastructure and Information Technology within the KPPPA. In these circumstances, the company must be able to answer questions such as how it can happen? What will the company do? And others.

4.6.6 Risk Analysis

The use of information technology in the company is an important element to support the effectiveness and efficiency of the company's business processes. This information technology is expected by the company to improve service quality so that the achievement of the company's business objectives. The use of information technology must be accompanied by appropriate and relevant management to minimize the risks that may arise in the business process due to conditions outside the normal. Out-of-normal conditions are broadly divided into two things, namely:

1. The condition of the disaster, which is a condition outside the normal that has a broad impact, so that practically more than 70% of the infrastructure needed to conduct business information technology services.
2. The condition of non-disaster (isolated), is a condition outside the normal that has an impact that can be isolated, only less than 30% of the infrastructure supporting the information technology service business is affected.

This condition requires identification and risk analysis to determine the classification of the impacts and causes of possible disaster events. Every source of the disaster carried out a risk analysis and handling and determined the person in charge of each event, as explained below.

4.6.6.1 Emergency Response to Disaster Conditions

Emergency Response to disaster conditions must be handled directly by the KPPPA IT-DRP Team in coordination with the IT Data and Management Section. The disaster conditions here are defined in two types: natural disasters (Environmental Disaster) and human-caused disasters (Organized Disaster). These are shown in Table 1 and Table 2.

Table 1 Environmental Disaster

Scenario	Person in charge
Flood - the scenario has been made	• IT-DRP / BCP Team • Data Section • IT manager
Earthquake - the scenario has been made	• IT-DRP / BCP Team • Data Section • IT manager
Fire - the scenario has been made	• IT-DRP / BCP Team • Data Section • IT manager

Table 2 Organized Disaster

Scenario	Person in charge
Act of terrorism -the scenario has been made	• IT-DRP / BCP Team • Data Section • IT manager

4.6.6.2 Emergency Response to Non-Disaster Conditions

The Emergency response of non-disaster conditions is not required to handle a special team, only to be handled by related functions. Table 3, 4, and 5 show the intended scenario.

Table 3 External Infrastructure Outage

Scenario	Person in charge
Normal Electricity Failure (Electrical Power Failure) -the scenario has been made	Head of Logistics / Household Section
Communications services breakdown -the scenario has been made	Head of Logistics / Household Section

Table 4 Internal Infrastructure Outage

Scenario	Person in charge
Internal power failure -the scenario has been made	Head of Logistics / Household Section
AC Failed On (Air conditioning failure) -the scenario has been made	Head of Logistics / Household Section

Table 5 Information and IT Incident

Source of Conditions Outside Normal	Person in charge
Lost Data and Information Records - the scenario has been made	• Data section • IT manager
Error disclosure of information -the scenario has been made	• Data section • T manager

Source of Conditions Outside Normal	Person in charge
The IT system failed to operate -the scenario has been made	• Data section • IT manager
Network Outage -the scenario has been made	IT manager

4.7 Develop and Implement Planning Testing, Training, and Training.

Hold training to prepare recovery personnel to activate plans to improve the effectiveness and readiness of the overall disaster recovery team.

4.6.1 Preparedness

As explained in the previous sections, this document is related to other documents in the KPPPA. Therefore, periodic monitoring and evaluation must be carried out; as a whole, the linkages between these documents can be maintained, and all supporting facilities/infrastructure can be maintained when needed. In this section also will be explained about the testing method that must be done to be still able to maintain the preparedness of all related elements in this IT-DRP document.

4.6.2 Monitoring

The monitoring activity includes the following:

1. Monitoring the validity of these IT-DRP documents along with all documents that become references and other related documents. This monitoring is done at least once every year.
2. Monitoring the functioning of this IT-DRP supporting infrastructure, as follows:
    a. IT facilities at the KPPPA are monitored regularly.
    b. The existence of a copy (copy) IT Disaster Recovery Plan Document this in the following places, performed at least every two times in one year.
        i. IT Operational Location under normal conditions.
        ii. Command Center Location
        iii. IT-DRP Location
3. Fire handling facilities, such as:
    a. Checking the function of each Light Fire Extinguisher (APAR), carried out at least once in a month.
    b. Checking the functioning of the building hydrant system installation, carried out at least once in five years.
    c. Checking the functionality of the FM-200 installation is carried out at least twice a year.
    d. Checking the function of smoke detectors is carried out at least once a year.
    e. Testing the function of fire alarms is carried out at least once a year.
4. Electrical support facilities, such as:
    a. Checking the functioning of the generator set is done at least once a week.
    b. Checking the building's electrical installation is carried out at least once in 5 (five) years.
    c. Checking the installation of clean water and building dirty water, carried out at least 1(one) time in each

d. Checking the building's lightning rod installation is carried out at least once in every 5 (five) years.

4.7.3 Testing

Testing related to the IT Disaster recovery plan was carried out to ensure that this plan can be implemented, related personnel can implement this plan, and awareness of all KPPPA employees on business continuity can be well maintained.

Conducting testing aims to determine the deficiencies contained in the DRP when IT-DRP is implemented. Each component of the information system must be tested to ensure the accuracy of the recovery procedure. The following fields must be considered in the ITDRP test as applicable Notification procedure.

1. System recovery on alternative platforms from backup media
2. Internal and external connectivity
3. System performance using alternative equipment
4. Normal operational recovery
5. Testing other plans that affect IT-DRP

Periodically testing IT-DRP and/or if there are major/minor changes. Tests are carried out with strategies in accordance with NIST standards 800-34 with the following principles.

1. Perform tabletop testing (in the form of joint discussions from the IT-DRP team and the Data Field leadership structure related to aiming to verify and validate the adequacy of information based on scenarios outside normal conditions (both disaster and non-disaster) defined in this document, which is done at least once a year.
2. Conduct drill / real simulation carried out based on scenarios of abnormal conditions (both disaster and non-disaster) defined in this document, which is carried out at least once in every 3 (three) years. With this practice, it is expected that the personnel can be accustomed to emergency conditions so that when the actual emergency occurs, they can be ready to handle it.

4.7.4 Training and Building Awareness

Conduct training for personnel involved in IT-DRP to familiarize them with the role they play in IT-DRP to work effectively.

This approach helps the staff to be ready when the disaster occurs. Recovery training must be based on the following elements:

1. The purpose of IT-DRP
2. Coordination and communication between teams
3. Reporting procedure
4. Security requirements
5. Specific team activities (activation, recovery, and reconstruction)
6. Individual responsibility (activation, recovery, and reconstruction)

Awareness and training on IT Disaster recovery plan carry out periodically to ensure the level of skill of personnel. They can be done in class or simulations in the field.

4.8 Planning treatment.

The plan should be a document that is updated regularly in accordance with the increase in information technology systems and environmental organizations using periodic review. The results of the IT Disaster recovery plan testing must be outlined in an official report addressed to Top Management at the KPPPA. IT Disaster recovery plan reviews are carried out every time after testing, to ensure that this document can guarantee business continuity under any circumstances. If the results of the review require an update/change to the IT Disaster recovery plan, then it must be done based on the process of changing the official document of the organization. In this case, the Ministry of PPPA and must be re-socialize to the parties related to the results of the changes.

5. Conclusions

Based on the discussion, it can be concluded that the Indonesian KPPPA:

1. Can design a DRP IT model that is made periodically and integrated.
2. Have to implement IT DRP based on the design that has been done.

Bibliography

[1] Ulum, Mochamad Chaezienul. “Governance dan Capacity Building Dalam Manajemen Bencana Banjir di Indonesia.” *Jurnal Penanggulangan Bencana* 4.2 (2013): 5-12.

[2] Jakarta berpotensi diterjang tsunami, taken from: https://www.suara.com/wawancara/2018/04/09/102546/widjo-kongko-jakarta-utara-juga-berpotensi-diterjang-tsunami accessed Desember, 15 2018 time 10.20 WIB

[3] Nguyen, Ngoc, et al. Indonesia’s Historical Earthquakes: Modelled Examples for Improving the National Hazard Map. Geoscience Australia, 2015.

[4] Koulali, A., et al. *The kinematics of crustal deformation in Java from GPS observations: Implications for fault slip partitioning.* Earth and Planetary Science Letters 458 (2017): 69-79.

[5] Seminary Result of BMKG taken from http://www.bmkg.go.id/Berita/?p=seminar-ilmiah-sumber-sumber-gempabumi-dan-tsunami-di-jawa-bagian-barat&lang=ID accessed Desember 24 2018 time 15.27 WIB

[6] Toigo, Jon William. Disaster recovery planning: Preparing for the unthinkable. Prentice Hall, 2003.

[7] Template Document NIST, taken from https://www.nist.gov/ accessed Desember 11 2018 time 16.15 WIB

[8] Kaligis, Otto Cornelis. Penerapan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Dalam Prakteknya. Yarsif Watampone, 2012.

[9] Indonesia, Peraturan Pemerintah Tentang Penyelenggaraan Sistem, and Transaksi Elektronik. "Nomor 82 Tahun 2012." LN Tahun 189 (2012).

[10] Regulation of the Minister of Women Empowerment and Child Protection of the Republic of Indonesia (PERMENPPPA) Number 3 ear 2018 About the Implementation of Information Technology in the Ministry of Women's Empowerment and Child Protection.

[11] Information Technology Strategic Plan 2015-2019 the Ministry of Women's Empowerment and Child Protection.