RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES

Social Science Journal

# Disaster Recovery Design at Higher Education InstitutionUsing ISO 27031 Method

By

**Johanes Fernandes Andry**
Information Systems Department, Universitas Bunda Mulia, Indonesia
Email: jandry@bundamulia.ac.id

**Hendy Tannady**
Department of Management, Universitas Multimedia Nusantara, Indonesia
Email: hendy.tannady@umn.ac.id

**Glisina Dwinoor Rembulan**
Department of Management, Universitas Bunda Mulia, Indonesia
Email: grembulan@bundamulia.ac.id

**Gerry**
Information Systems Department, Universitas Bunda Mulia, Indonesia
Email: gerryy720@gmail.com

**Honni**
Information Systems Department, Universitas Bunda Mulia, Indonesia
Email: honni@bundamulia.ac.id

## Abstract

Object of this research which is one of private university in Indonesia realizes their need for a continuous control effort to maintain their business continuity. An IT implementing increased risk at University is closely related to this control effort, especially for academic institutions, student, teacher, lecturer data or financial data are the most important data for a university. A negative impacts that risk have can cause a disaster because of the its potential to threaten the organization's business activities sustainability that reach a certain criteria. This is what encourages the University to prepare itself for possible disasters. This research objective is to prepare University's Disaster Recovery Plan (DRP). A type of contingency plan that includes contingency strategies preparation, preventive controls identification, Business Impact Analysis (BIA), response and preparation to an organization when a disaster happen. The result of this research is a DRP document adapted to the conditions of the organization. The DRP document contains guidelines for preventive measure and service recovery before happen.

**Key words:** Disaster, Risk, Disaster recovery plan, Information Technology

## Introduction

Information technology (IT) is a set of tools and information used to help complete work by processing interconnected information [1]. BCM (Business Continuity Management) is an improvement in strategies, plans, and a response taken in preparing resilience to provide protection to business operational processes if operational processes are interrupted, and to protect from serious or potentially damaging losses to the company [2][3].

Apart from BCM the IT system has become vital for every business aspect [4]. The IT DRP is required to have requirements and steps that can be applied to a company in managing disasters that may occur and can affect the IT system at the University. The main objective of a disaster recovery plan is to provide resources to restore the basic business so that it can be temporarily backed up and can be continued until the system returns to normal and functions as before the disaster [5]. The purpose of planning DRP is to ensure that critical business operational processes are protected in the event of a disaster [6]. It is an effective way to solve IT system's problem. To restore all business process framework in the company, an organization must have a DRP after disaster happen. [7]

The Disaster Recovery Plan (DRP) will produce a document result. This document will be the main source if someday there will be an emergency when a disaster occurs and about the IT system. To recover everything that lost in the IT system, the DRP will provide a procedure. Therefore, the document must be detailed, simple, and readable. This document objectives must be stated clearly in introduction. The stages of DRP preparation begin with identification and risk assessment to determine the patterns of risk that threaten the sustainability of IT services at University. After knowing the existing risk patterns, then the research is continued by determining the priority of IT service recovery through a Business Impact Analysis (BIA). This guide will provide direction regarding the rules and platforms behind the task information and communication technology (ICT) while ensuring the continuity of business operational processes. The International BCM (Business Continuity Management) standard developed by ISO 27031 summarizes the BCM approach to preventing, reacting and recovering from incidents.

The activities involved in BCM are DRP, management of operational continuity, incident preparedness, and focused risk mitigation increase the strength of an organization and prepare it to react effectively to incidents and restore the predetermined time frame [8]. Based on its responsibilities, the unit is the information storage and center of all important data that must be maintained to make sure University system keep run.

## Literature Review

### *2.1 Business Continuity Planning*

Means "the effort to carry out comprehensive management to prioritize key business processes and define normal operations and develop mitigation strategies to ensure that the organization responds effectively and efficiently to challenges during and after a crisis" [9]. According to [10] the ultimate goal of a business plan is to prepare for disaster recovery and is to make sure an organization can survive. Business continuity plan. In recent years, the BCP has become an important part of the management plan. By introducing "corporate risk that allows the company to continue to operate in adverse conditions." An appropriate continuity of business and plan of crisis management, recovery objectives, and resilience strategy [11]. Define the business continuity plan as the "criterion for proactively identifying risks and vulnerabilities, and Plan in advance how to reduce, accept or distribute them during a business disruption.

### *2.2 Disaster Recovery Planning*

The US Federal Emergency Management Agency [12]. Defines a DRP. Disaster recovery is a non-emergency action after a disaster, the goal of which is to restore all systems to be as normal as possible, whether it is a informal or formal systems. Steps the organization should take during and immediately after a disaster. The Company's Sustainable Development

Plan outlines the disaster recovery plan and continues the disaster recovery plan. Continue operations after a disaster.

### *2.3 ISO 27031*

Describes the principles and concepts of compiling information and information communication technology (ICT) to achieve continuity of a business and provision identify and define various aspects (such as performance standards, design, and implementation) to increase the level of the organization's ICT preparation to ensure continuity business [13]. This One Applies to any of the following organizations (regardless of size, private, governmental and non-governmental organizations) Setting up an ICT for business continuity plan (IRBC) and requires information and communication technology services / infrastructure to support business operations at all times. Incidents, incidents and related disruptions, these can affect the continuity of critical business functions (including security). It also allows organizations to measure parameters of performance related to their online IRBC Consistent and recognized. It extends and contain the information security incident management and handling practice, as well as ICT preparation and services[14].

## 3. Methodology

Data and information about the development unit of information and communication technology through direct discussion, interview, and observation with related experts. The investigation stage is carried out by using the literature related to the research. Conduct literature research by reading journals and book that contains planning disaster recovery theories and gathering information resources via internet. Select ISO27031is a method that used un this study. This method was chosen because it has the following advantages 1) ISO is a standard Scope ranges from medium to upper, 2) Its suitable in IT management used, 3) A IT management framework that can be used to manage the infrastructure of information and technical in an organization and the way of providing services most suitable for IT users, 4) At the organization’s highest level, it can helps to fulfill and achieve their legal, ethical, and regulatory requirements in terms of the use of IT organizations [15].

DRP design begins with a current systems analysis and also internal and external threats identification. After get a risk assessment, one step further in the risk management process is carrying out a risk analysis to determine each risk level[16].

The level of risk is determined using the analysis of effect and failure mode (FMEA) method [17]. Then BIA is carried out. The systematic process of identifying and evaluating the potential impact of disruption to critical business operations resulting from a disaster, accident or emergency [18]. To get an evaluation of system administrators opinion, and important assets units in the IT Development Unit and University spread. At the same time, quantitative analysis is used to evaluate the productivity of existing systems. Two important parameters of a recovery plan whether data protection and calculating disaster in terms of quantitative methods is Recovery Time Objective (RTO) and point recovery objective (RPO)[19]. The plan of disaster recovery content design is based on ISO / IEC 27031 standards. At the end, the process of validation is done by the stakeholders of University’s Unit of Communication and Information Development Technology to prove that unit needs already fulfilled by the DRP documents.

## 4. Analysis and Discussion

This section explains that every stored data must be backed up to reduce the occurrence of permanent data loss. There are many ways to back up, just choose from the owner you want to back up with what method. Then the last risk validation as an agreement that the design of this disaster is agreed upon by several parties responsible for this design. At this stage, the identification of risks from the theory that threatens the University information system specifically is carried out.

The authors already verified and validated the risks that obtained from the literature. In this verification and validation, experts can add, subtract and increase points of risk data so that they are relevant to the University's Unit of Communication and Information Development Technology. Furthermore, the researchers grouped the data on the severity / impact of the disaster indicators that would occur. In this grouping the researcher measures the level of danger, explanation, and time-consuming risk arising from these indicators as well as the severity from 1 to 10 which will be shown in table 1. In this grouping, the researchers used previous research from several experts as a guide to measure the severity and impact of the disaster indicators if they happened at University.

**Table 1.***Table of Level for Occurrence*

| Level - Effect | Information | Time is cut (Hours) |
|---|---|---|
| 10 - Dangerous without change | Can break servers without warning | > 6 x 24 |
| 9 - Dangerous but there is a warning | Can compromise servers with advance warning | > 5 x 24 -> 6 x 24 |
| 8 - Very high | Failure to completely disrupt the server | > 4 x 24 -> 5 x 24 |
| 7 - High | Failures disrupt 50% of server work | > 3 x 24 -> 4 x 24 |
| 6 - Medium | Failures disrupt 25% of server work | > 2 x 24 -> 3 x 24 |
| 5 - Low | Failures disrupt 10% of server work | > 24 -> 2 x 24 |
| 4 - Very low | Failure affects server work | > 12 -> 24 |
| 3 - Small | Failures have little effect on server failures | > 6 -> 12 |
| 2 - Very small | has a negligible effect | > 3 -> 6 |
| 1 - There is no | Failure has no effect | > 0 -> 3 |

BIA is the next stage, which was a stage to determine the values of RPO and RTO for each critical server in the University's Unit of Communication and Information Development Technology. RTO value was needed to know how long cut off on a server during repairing when a disaster happen that cause the server to be cut off. Table 2 is show the RTO assessment.

The RPO assessment is to know, when a disaster happen, how much data will disappear. This values is really vital on the server backup method in the University's Unit of Communication and Information Development Technology. Table 3 is show assessment of the RPO.

A distributing questionnaires is determined both, RPO and RTO values. This distributing questionnaires was filled by one person from each division, that is the multimedia division, collection division, and network division. Three people will get the questionnaires with the aim an accurate data obtaining about the state of the University's Unit of Communication and Information Development Technology. Observe the time of server was disconnected, is the way to know how critically the serves was.

**Table 2.** *RTO Assessment (Hours)*

| RTO is a time of user's loss tolerate before the application use is regained. | |
|---|---|
| 0 | 0 hours |
| 1 | 24 hours |
| 2 | 48 hours |
| 3 | 72 hours |
| 4 | More than 72 hours |

In planning DRP, to maintain the data security, a backup of data location is needed . The location indicator refers to ISO 27031, which is compared with the conditions at each location.

**Table 3.** *RPO Assessment*

| RTO is is a time of user's loss tolerate before the application use is regained. | |
|---|---|
| 0 | No data is allowed to be lost |
| 1 | In the last 8 hours regardless of when the disturbance occurred |
| 2 | All data entered since the last backup must be re-inputted |
| 3 | It can take up to one week of lost data to be reconstructed |

Alternative locations and considerations in server creation can be reviewed from University itself, whether you want to store it in the cloud or rent out a place in the data center or even build your own server location, which is important in making this backup server location, you must pay attention to several things, namely:

***The availability of electricity for data center operations***

The sharp increase in electricity consumption has led to frequent blackouts in some countries with poor infrastructure. The data center requires a very large amount of electricity, and even a momentary blackout can cause the data center to not operate even for a moment.

***Cooling system and climate***

Having many computers in one room generates heat, and cooling them can be very expensive. Data centers built in cool and cool climates can reduce costs because the outside air can be used to cool them.

***Risk of disaster***

Data centers must be built in places / locations that have minimal risk of disasters such as floods, earthquakes, and others; not built that are high below sea level or through the flight path but if you want to avoid that all can be stored in the cloud.

***Data Security (data security)***

Concerns about privacy and data confidentiality are also taken into consideration. The existence of a state regulation that can view / collect data stored in a data center is a threat to corporate companies against the security of the data they store.

The DRP document's draft for the University's Unit of Communication and Information Development Technology refers to ISO / IEC 27031. The DRP Document's standard content must be contained regulation from ISO / IEC 27031 as follows; Team of Recovery Application, Plan of Recovery and Response, Call Plan, responsibilities and roles, scope and purpose. In order to competent personel can use it when incident happen, the plan must be documented. Overall framework must be define in documentation in which a plan of recovery is prepared, includes the team of recovery and their responsibilities while and after an incident happen, Timeline for recovery, Critical services based on RPO and RTO values, and Overall strategy. Documentation consists of Purpose, Coverage based on BIA, Availability requirements defined by the business for the availability of related technologies and services, requirements of information technologies, attachments. Attachments consist of a database, application, systems of inventory information; network infrastructure servers and review; Inventory of software and hardware systems; agreements and service level contracts. Finally, documentation of the major ICT suppliers. The validation of document is carried out after the DRP document design. The chairman of the University's Unit of Communication and Information Development Technology is the one who approved this document. The validation result is that the DRP document is designed accordance with the unit's need. The draft of this document is based on ISO / IEC 27031. Then, the document validation is carried out and validated by the Chairman of the University's Unit of Communication and Information Development Technology, Network Division, and Multimedia Division, and the result is the DRP document is designed accordance to the unit's need.

## 5. Conclusion

This study already developed a DRP document for data systems in the University's Unit of Communication and Information Development Technology. The DRP document consists of quick response activities and also procedures when disaster happen. While a disaster happen, this document will be used. There is a analysis of risk at DRP document. It analyzes data systems' potential damage using the FMEA method. This document also has RPO and RPTO values which will be used to store location and system of the backup services that can be used later as a backup when the main server being repaired. Suggestions for further research on DRP include documents and also cost money.

## References

F. Nurprihatin, E. L. Jayadi and H. Tannady, "Comparing Heuristic Methods' Performance For Pure Flow Shop Scheduling Under Certain And Uncertain Demand,"Management and Production Engineering Review, vol. 11, no. 2, pp. 50-61, 2020.

F. E. Gunawan, J. F. Andry, H. Tannady and R. Meylovsky, "Designing Enterprise Architecture Using TOGAF Framework in Meteorological, Climatological, and Geophysical Agency,"Journal of Theoretical and Applied Information Technology, vol. 97, no. 20, pp. 2376-2385, 2019.

J. S. Patel and K. V, "Disaster Recovery in Business Continuity Management," Int. J. Trend Sci. Res. Dev., vol. Volume-3, no. Issue-4, hal. 319–322, 2019.

D. Elliott, Business Continuity Management. 2001.

E. Makwae, "An assessment of disaster recovery planning: A strategy for data security," Researchgate, no. September, 2018.

S. Adedayo, "Disaster Recovery Strategy and Maintenance Plan Network Management Using Cyberoam View project," Researchgate, no. October, hal. 2016, 2014.

J. Fenton, "Business Continuity and Disaster Recovery," Audit. Cloud Comput. A Secur. Priv. Guid., hal. 129–141, 2011.

H. Tannady and E. Purwanto,"Quality Control of Frame Production Using DMAIC Method in Plastic PP Corrugated Box Manufacturer," Annual Conference on Science and Technology Research (ACOSTER) 2020, Journal of Physics: Conference Series, 2021.

J. Watters, "Disaster Recovery, Crisis Response, and Business Continuity: A Management Desk Reference," 1390.

E. D. Madyatmadja, Marvell, J. F. Andry, H. Tannady and A. Chakir, "Implementation of Big Data in Hospital using Cluster Analytics,"2021 International Conference on Information Management and Technology (ICIMTech), AIP Conference Proceeding,Jakarta, Indonesia, 2021.

International Standard Organization, “INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Application security —,” vol. 2011, 2011.

J. F. Andry, L. Liliana, A. Chakir and H. Tannady,"Online Voucher E-Commerce Testing Using ISO 9126 Model,"2021 International Conference on Industrial, Enterprise, and System Engineering (ICOIESE), AIP Conference Proceeding, Bandung, Indonesia, 2021.

C. K. Hughes, “Disaster Recovery Planning,” Das Rechenzentrum, vol. 8, no. 4, hal. 236–239, 1985.

J. F. Andry, H. Tannady, I. I. Limawal, G. D. Rembulan and R. F. Marta, "Big Data Analysis On Youtube With Tableau,"Journal of Theoretical and Applied Information Technology, vol. 99, no. 22, pp. 1915-1929, 2021.

D. Meilani, I. Arief, dan M. Habibitullah, “Designing Disaster Recovery Plan of Data System for University,” IOP Conf. Ser. Mater. Sci. Eng., vol. 697, no. 1, 2019.

E. D. Madyatmadja, L. Liliana, J. F. Andry and H. Tannady, "Risk Analysis of Human Resource Information Systems Using Cobit 5,"Journal of Theoretical and Applied Information Technology, vol. 98, no. 21, pp. 3357-3367, 2020.

A. Lobodally, “The Commodification of DIsaster in Telkomsel TVC "Menjadi Relawan Yang Terbaik" Version,” Advances in Social Science, Education and Humanities Research (ASSEHR), vol. 208, 2018.

H. Sutopo and A. D. Astono, “Developing Digital Magazine on Coffee Industry Information in Covid-19 Pandemic for Tourism Enhancement,” 5th International Conference on Computer Science and Artificial Intelligence, pp. 352-358, 2021.