p-ISSN 0853-7720; e-ISSN 2541-4275, Volume 7, Nomor 2, halaman 321 – 334, Juli 2022
DOI : http://dx.doi.org/10.25105/pdk.v7i2.7082

JURNAL
PENELITIAN DAN KARYA ILMIAH
LEMBAGA PENELITIAN UNIVERSITAS TRISAKTI
https://trijurnal.lemlit.trisakti.ac.id/lemlit

RISK ASSESMENT AND BUSINESS IMPACT ANALYSIS AS A BASIS FOR THE DRAFTING DISASTER RECOVERY PLAN AT UPT-TIK OF XYZ UNIVERSITY

Laqma Dica Fitrani[1)]

[1] Informatics Department STIE Perbanas Surabaya

*Correspondent Author: laqma.fitrani@perbanas.ac.id

ABSTRACT

Disasters can come at any time, cannot be determined when, how they occur, how long and how big the impact they have. Disaster Recovery Plan is a plan prepared by the organization in dealing with disasters, the procedures and what steps must be carried out is described in this document. As the basis for the drafting of the document, two important things are required including several risk assessments which analyze all possible threats and business impact analysis which analyze the impact of the disasters on business activities in an organization. This research was conducted at UPT-TIK (Technical Implementation Unit of Information and Communication Technology) of XYZ University. The results of this study were the risk assessment and business impact analysis which form the basis of the drafting of disaster recovery plan document which include the team responsible for disaster recovery planning.

SEJARAH ARTIKEL

Diterima
……..20…
Revisi
…….. 20…
Disetujui
…….. 20…
Terbit online
…….. 20….

KEYWORDS

- Business Impact Analysis,
- Disaster Recovery Planning,
- Risk Assesment

1. INTRODUCTION

Business are becoming increasingly dependent on information technology to improve operations and provide competitive advantages (Bhatt, 2005). Strengthening information technology is very important because most businesses cannot continue to operate successfully if their information technology services are not available (Bradburry, 2008).

In this Internet era, the Internet Data Center (IDC) has emerged as a major network service platform to unify internet services into one location and offer more efficient data center services for

p-ISSN 0853-7720; e-ISSN 2541-4275, Volume 7, Nomor 2, halaman 321 – 334, Juli 2022
DOI : http://dx.doi.org/10.25105/pdk.v7i2.7082

an institution or company. IDC manages servers and networks along with important and sensitive data.

XYZ University is one that applies open and distance learning system. This learning system has proven to be effective in increasing coverage and equal distribution of quality higher education opportunities for all Indonesian citizens, including those who live in remote areas, both throughout the country and in various parts of the world. This wide coverage makes XYZ University has a lot of students, amounting to 292,465, so that adequate information storage is needed in the data center.

As a data processing center, the data center stores company information including sensitive and critical information. As a result, data center needs physical and logical protection to secure information systems from attacks that threaten the security.

In the management of organization, risk issues are often not a concern of the management. Whereas in the concept of sustainable management an organization was established with the assumption to continue operating for an unlimited period of time. Risk is often a limiting factor in an organization's operations to achieve goals. When an incident or disaster occurs, the organization will suffer losses in general. These losses include: inaccessible information (loss of availability), corrupted data or has been turned into waste data (loss of integrity) and there might be a leak of important information that should be protected (Tripton, 2006). A good IT management is able to minimize these risks by providing appropriate treatment of the possible risks so that the business can continue running smoothly (Kaplan, 2012).

The potential for disasters in Indonesia is relatively high, this means that natural disasters have continued to increase, regardless of the unforeseen minor disasters (human error, system failed, etc.) in the past 10 years. For XYZ university, natural disasters can disrupt the continuity of the direct information and data services so that if natural disasters or minor disasters occur, it creates a high risk.

The dynamic environment is unpredictable, thus a disaster cannot be denied. Saving the data and information stored in data center in the form of an application server and supporting facilities is very important because it will affect the level of service and information provision at XYZ university, so that data redundancy or disaster recovery planning needs to be prepared by considering disasters including natural disasters such as earthquake, tsunami, volcanic eruption which may be caused by geographical conditions, and human-caused disasters such as building failures, fires and other environmental factors. Therefore, making a disaster recovery plan (DRP) for IT systems that support business needs is very important to do (Hayes, 2005).

p-ISSN 0853-7720; e-ISSN 2541-4275, Volume 7, Nomor 2, halaman 321 – 334, Juli 2022
DOI : http://dx.doi.org/10.25105/pdk.v7i2.7082

Seeing the great potential and the need for DRP, especially for XYZ university, the authors use this research to create a DRP model that suits the needs of XYZ university.

2. LITERATURE RIVIEW

A. Previous Research

Previous research had been carried out by King and friends entitled "Lessons of Disaster Recovery Learned for Information Systems Management in US Higher Education" (King, 2010). The results of the study were the impacts of disasters that have occurred in the United States within a period of 15 years in several tertiary institutions, these results became the basis of the importance of a plan in dealing with the danger of a disaster, in that study the discussion was very general and not explained about risk assessments, whereas risk assessment is an important process in determining which threats are critical and which one's are not, as a basis for developing disaster recovery strategies in the DRP document.

B. Disaster

Disasters are business disruptions resulting from "terrorist attacks, power outages, security breaches, traits and human error (Decker, 2005).

In general, in terms of information technology environment, disaster is described as an event that results in significant disruption to the daily information technology capabilities of the business. Examples of such incidents include damage to critical IT components, lack of access to data centers or personnel issues that cause reduced support for production.

Table 1. Classification of Disaster

Classification	Description
A	Total damage to the critical business systems or networks that cannot be repaired in the required time. **and/or** Damage to the data center resulting in inaccessible facilities or cannot be used **and/or** Injured personnel or situations that prevent IT personnel from carrying out their duties for a long time.
B	Damage to the data center that does not result in the closure of the data center **and/or** Partial damage to the critical business systems that is expected to be recovered in the required time
C	Damage to the isolated critical systems / networks or total / partial damage to non-critical systems / networks. This kind of damage has no effect on critical systems or can certainly be restored within the required time.

p-ISSN 0853-7720; e-ISSN 2541-4275, Volume 7, Nomor 2, halaman 321 – 334, Juli 2022
DOI : http://dx.doi.org/10.25105/pdk.v7i2.7082

C. Disaster Recovery Plan

Disaster Recovery Plans are procedures to respond emergencies, providing long-standing backup operations during interruptions, and managing the recovery and rescue processes afterwards, companies must have good skills in handling data losses (Ronald, 2011).

Disaster recovery plan refers to preparations for dealing with disasters and responses that must be given when a disaster occurs. the purpose of the DRP is the continuity or the ability of an organization to survive in dealing with disasters (Peter, 2007).

The Disaster Recovery planning key elements and supporting best practices that are identified within this study are organized into a five-stage process. This process can be used to guide the efforts of IT professionals, as well as other individuals who are involved in DR planning, in the identification of risks that face an organization's time-critical IT systems and the development of an explicit strategy to address those risks.

3. RESEARCH METHODOLOGY

In drafting this disaster recovery plan the authors used several stages, namely (Sneadaker, 2010):

1. Project Initiation

   Stage to determine the needs and objectives of the drafting of disaster recovery plan (DRP)

2. Risk Assessment

   Risk assessment is used to determine the possible threats and the associated IT system risks. The output of this process is the ability to identify appropriate controls to reduce or eliminate risk during the risk mitigation process. To determine the likelihood of future events, threats to IT systems must be analyzed in relation to the potential vulnerabilities. Impact refers to the magnitude of the danger that can be caused by vulnerability. The level of impact is regulated by the potential impact and the impact affects the IT assets and resources.

3. Business Impact Analysis

   Important components of an organization's business impact analysis (BIA) include an exploration to find out vulnerabilities and a planning to develop strategies in minimizing risks. The result of the analysis is a business impact report that illustrate the potential risks to an organization. One of the basic assumption behind BIA is that each component of the organization depends on the continued function of every other component. Risks contained in Data Centers and Networks will later be analyzed based on the existing business impacts.

p-ISSN 0853-7720; e-ISSN 2541-4275, Volume 7, Nomor 2, halaman 321 – 334, Juli 2022
DOI : http://dx.doi.org/10.25105/pdk.v7i2.7082

4. DRP Development

   Developing a draft or document of disaster recovery plan.

4. RESULT AND DISCUSSION

A. Scope and Principles of Planning

This Disaster Recovery Plan was prepared following the principles of planning, where various scenarios must be considered to form a planning basis, and various assumptions were made to anticipate the future events and the required needs. The use of this plan was predicted in several main principles, namely:

a. XYZ University will use alternative locations and information system resources to restore the functionality of related systems during an emergency situation that prevents access to the key facilities;
b. Computer systems that have been determined at alternative locations have been configured in accordance with the requirements of processing related information systems;
c. Alternative locations will be used to continue the recovery and information system processes during the period of disruption, until returning to normal operation;
d. The information system cannot operate at XYZ University's Data Center facilities and cannot be restored for 1 to 6 hours;
e. Key personnel who maintain and operate established systems have been identified and trained in terms of the response to emergencies and their role in the recovery process; they are available to activate the Contingency Plan for specified systems;
f. Preventive control equipments such as generators, fire extinguishers, air conditioners, and environmental control devices run normally when disaster occurs;
g. Data Center equipments include the supporting information system components connected to the UPS which provides power supply for at least 60 minutes during the power supply disconnection.
h. The hardware and software for the specified information systems, which are operated at XYZ University Data Centers are not available / not operating for 1 to 6 hours (depending on the application of Maximum Allowable Outage ("MAO");

p-ISSN 0853-7720; e-ISSN 2541-4275, Volume 7, Nomor 2, halaman 321 – 334, Juli 2022
DOI : http://dx.doi.org/10.25105/pdk.v7i2.7082

i. The latest backup of each application software and complete data is available at the offsite storage facility;
j. The devices, connections and capabilities needed to operate the specified information systems are available at the Disaster Recovery Center;
k. Service agreements for the hardware and software of the specified application systems are well maintained to support emergency system recovery.

In order to reduce the possibility of disaster, several steps have been implemented, one of which was the preparation of facilities and infrastructure to support the Data Center. The following items are the readiness of supporting facilities for XYZ University Data Center:

1. Data center room
   a. Data Center already has room for servers and power equipped with an integrated air cooling system. The operator workspace is separate from the server and network equipment room, but still in a nearby location.
   b. Wiring for power and network has been put in a special lane. Network wiring that enters the Data Center room uses the floor track ladder cabling, while the power wiring line uses trays.
   c. Raised floor is equipped with detection devices that are capable of detecting puddles of water and smoke.
2. Data center room's air conditioning
   a. To achieve the operational temperature of the Data Center room which is in the range of 18^{o}C (18 degrees Celsius) and the operational humidity of the room which is in the range of 60%, the UPT ICT Data Center is equipped with 2 (two) central cooling units and 3 portable cooling units that control temperature and also Data Center humidity.
   b. At normal Data Center workloads, the two cooling units that work to maintain the floor track ladder cabling temperature and humidity are in the Data Center room, where the two central cooling units are backing each other up, and if the two units do not function then the 3 portable cooling units will be used.
   c. The storage locations of 2 (two) cooling units in the Data Center engine room are evenly distributed as well as for the 3 portable cooling units.

p-ISSN 0853-7720; e-ISSN 2541-4275, Volume 7, Nomor 2, halaman 321 – 334, Juli 2022
DOI : http://dx.doi.org/10.25105/pdk.v7i2.7082

3. Data center room's power supply
   a. The UT Data Center gets the power supply from the BAUSI LP Building, PUSKOM, for servers and server equipments, of 88 kVA.
   b. The power input from the PLN is connected to 8 (eight) UPS units, each consisting of 4 Primary UPS and 4 Secondary UPS with a capacity of 55 kVA each.
   c. The four 55 kVA Primary UPS units can supply for 20 minutes at normal load and the four 55 kVA Secondary UPS units are able to supply for 20 minutes at normal load.
   d. The operating expenses of the UPS each reached 40%.
   e. The power supply from PLN uses 2 different substations, so when 1 substation dies, there is still 1 other substation.
   f. The power supply of the UT comes from the PLN power supply and also the backup generator.
4. Internet network path to data center room
   a. The UT Data Center is connected to 5 (five) ISP backbones via Fiber Optic lines located at the UPT ICT, LPPMP building, XYZ University, with a bandwidth of 1 Gbps with the details of each ISP is 200 international Mbps, 200 local Mbps/IIX.

B. Risk Analysis

Risk analysis was carried out to determine the potential sources of disasters that will impact the Company's business processes. Below is a risk table that illustrates exposure and threat events.

Table 2. Disaster Potential

No	Threat	Affected Aspect		Event	Risk Control Options
		Information Capital	Human Capital		
1	**Natural Disaster**				
a	Epidemic of a disease		√	Never happened in the last five years	Health checks on leaders are carried out routinely once a year
b	Fire	√		Never happened in the last five years	Installation of fire prevention & control systems; Control and inspection of fire costs; no smoking in the data center.
c	Earthquake	√		Never happened in the last five years	Avoiding earthquake-prone areas for data center location if possible; building earthquake resistant structures for data center; installing stringer for high-pedestal raised floor
d	Volcanic eruption	√		Never happened in the last five years	Avoiding volcanic-prone areas for data center location if possible

p-ISSN 0853-7720; e-ISSN 2541-4275, Volume 7, Nomor 2, halaman 321 – 334, Juli 2022
DOI : http://dx.doi.org/10.25105/pdk.v7i2.7082

2	**Human Deeds**				
a	Transportation accident	√		Never happened in the last five years	Avoiding flight path areas for DC location
b	Management problems		√	Often happening	Conducting information security awareness training for leaders and employees
c	Employee error		√	Rarely happening	Conducting information security awareness training for leaders and employees
d	Processing information error	√		Often happening	Creating SOP for information processing
e	Misuse of access rights	√		Often happening	Creating SOP for acceess rights
f	Hacking	√		Often happening	Performing a regular penetration testing
g	Stealing	√		Rarely happening	Physical security: control access to data center facilities, security guards, surveillance systems using CCTV.
h	Threats and bomb attacks	√		Never happened in the last five years	Low profile facility, telephone number, not published
g	Stealing	√		Rarely happening	Physical security: control access to data center facilities, security guards, surveillance systems using CCTV.
h	Threats and bomb attacks	√		Never happened in the last five years	Low profile facility, telephone number, not published
i	Civil disturbance		√	Never happened in the last five years	Low profile facility, telephone number, not published
j	Malicious code, trojan, worm, backdoor, malware	√		Often happening	Installing anti-virus and anti-malware programs, providing awareness to users; opening a file or installing a program from an untrusted source.
K	Imperfect vendor services	√		Often happening	Applying NDA to employees of vendors
L	Viruses	√		Often happening	Installing anti-virus and anti-malware programs, providing awareness to users; opening a file or installing a program from an untrusted source.
3	**Technical Error**				
a	Application software failure	√		Often happening	Installing anti-virus and anti-malware programs, providing awareness to users; opening a file or installing a program from an untrusted source.
b	server malfunction/failure	√		Often happening	Set high availability cluster,backup hardware
c	DNS failure	√		Rarely happening	Set secondary DNS
d	Hardware failure	√		Rarely happening	Set high availability cluster,backup hardware
e	HVAC (Heating, ventilation, Air conditioner) failure	√		Rarely happening	Redundant HVAC system, perform routine HVAC maintenance
f	Power failure	√		Rarely happening	Redundant path power system;backup power generator, UPS
g	System software failure	√		Often happening	Conducting software testing, patch management
h	Telecommunications failure	√		Rarely happening	Routine maintenance schedule, establishing redundant telecommunication system

p-ISSN 0853-7720; e-ISSN 2541-4275, Volume 7, Nomor 2, halaman 321 – 334, Juli 2022
DOI : http://dx.doi.org/10.25105/pdk.v7i2.7082

C. Business Impact Analysis

Business impact analysis (BIA) used information generated by risk assessment that was the result of possible threats or risks analysis, then was linked to the activities or business processes that occur in the company. Therefore if the threat occurs on the company's activities, the impact on the company or customer can be determined. So this method can determine the main business processes that are sensitive to disaster threats.

Table 3. Critical Business Process

Risk Identification			Current Existing Control	Maintenance Plan
Asset Name	**Threats**	**Vulnerability**		
Server	Lack of Memory Capacity / HDD	Increased Data or Absence of Data Capacity Planning	Analyzing the needs of the used applications	Creating the data capacity planning
Domain / DNS	Procedures/rules abuse	Problems Cannot Be Resolved	Building awareness on procedures/rules for HR	Creating a socialization mechanism about information security awareness and socialization of existing rules, as well as creating a mechanism for monitoring its implementation
	Not resolve	The unknown period of Domain or Subdomain usage	Providing 2 domain servers	Creating domain usage monitoring
VLAN/Segmentation	Configuration error	Network not connected	Using a network monitoring system	Creating mechanism of network monitoring
Network provider services	Physical security	Lack of the division of physical security areas	There are no additional rules regarding the distribution of secure areas, public areas, and limited areas	Creating additional rules regarding the division of secure areas, public areas, and restricted areas
Antivirus	Got a virus or malware	Lack of regulations for the use of Anti-Virus	There are no additional rules related to the use of antivirus	Creating additional rules for antivirus usage
Linux & windows	Hacking	Patching is not performed	There are no additional rules related to patch management	There are no additional rules related to patch management
		Miss Configuration		Creating additional rules about software installation
Nginx & Apache	Hacking	No log management	There are no additional rules related to patch management	There are no additional rules related to patch management
		Patching is not performed		
Maria DB	Miss Configuration	System is not available	There are no inspection on the missconfiguration system	Performing penetration testing
Employer	Decreased work motivation		Recruitment procedures are the responsibility of the Personnel department	There is a background check mechanism and screening of the prospective employees
Log	Failure to identify information security disorders	Log is not complete	Log management is performed only on application error logs has not established log management software	Creating log management work instructions and monitoring the log

Current conditions that are related to disaster recovery site :

- The recovery site of the Data Center is currently located at the Multipurpose Building Data Center and Moratel Building (vendor);

p-ISSN 0853-7720; e-ISSN 2541-4275, Volume 7, Nomor 2, halaman 321 – 334, Juli 2022
DOI : http://dx.doi.org/10.25105/pdk.v7i2.7082

- Recovery site selection is the result of operational considerations based on existing conditions and practicality;
- Application systems are available at Data Centers which have a recovery strategy.

Table 4. Alternative Recovery for Applications

Application	Alternative IT Recovery Site	Operational Readiness	Ownership
Academic Site	UPT TIK	Hot site	Own
Teaching Material Site	UPT TIK	Hot site	Own
Report Site	UPT TIK	Hot site	Own
Support Site	UPT TIK	Hot site	Own
e-Learning	Cloud Azure	Cold site	Contrated site with Microsoft
Employee site	UPT TIK	Hot site	Own
Correspondence Site	UPT TIK	Hot site	Own

The critical applications, such the above table, is done by the hot site where the data is automatically copied to the second site in accordance with a predetermined recovery schedule. If the main server fails, then the second site will automatically replace it. Whereas e-learning applications are carried out in a cold site where recovery time cannot be predicted.

Table 5. The Needs of RTO and MTD for Applications

No.	Application Name	Scope	SLA	RTO	MTD
1.	Academic Site	National	Every day (24 hour)	10 Min.	2 days
2.	Teaching Material Site	National	Every day (24 hour)	25 Min.	2 days
3.	Report Site	National	Every day (24 hour)	30 Min.	2 days
4.	Support Site	National	Every day (24 hour)	10 Min.	2 days
5.	e-Learning	National	Every day (24 hour)	10 Min.	2 days
6.	Employee site	National	Every day (24 hour)	30 Min.	2 days
7.	Correspondence Site	National	Every day (24 hour)	25 Min.	2 days

The recovery strategy of each application is determined based on RTO and MTD. RTO is a maximum period of time needed to reactivate an application in the event of a disaster. While MTD is the maximum limit of recovery time for lost data or information.

p-ISSN 0853-7720; e-ISSN 2541-4275, Volume 7, Nomor 2, halaman 321 – 334, Juli 2022
DOI : http://dx.doi.org/10.25105/pdk.v7i2.7082

Table 6. Backup Strategies

Category	Server	*Backup Item*	*Backup Frequency*	*Backup Type*	*Backup Method*	*Off-site Storage*
Applications	Academic Site Teaching Material Site Report Site Support Site e-Learning Employee site Correspondence Site	*Application*	*Weekly*	*source & data*	*Only the latest changes/updates of the application* *Backup Tools*:	
		System Files	*Monthly and every time before maintenance / update shut down*	*Full*	*Backup Tools*: *OS-based backup* (Linux Tool). Using one tape for system files and binary; only the latest backup is saved.	*The backup results are not sent to the off-site*
	WEB SERVER	*Application*	*weekly*	*source & data*	*Only the latest changes/updates of the application*	
		System Files	*Monthly and every time before maintenance / update shut down*	*Full*	*Backup Tools*: *OS-based backup* (Linux Tool). Using storage sharing (FreeNAS)	*The backup results are not sent to the off-site*
		Binary (50-100MB)	*Monthly and every time when the system of file configuration changes*	*Full*	*External Harddisk*	*The backup results are not sent to the off-site*

D. Disaster Recovery Team and Responbilities

All individuals in the above source information environment should know who to find out or to be contacted when a potential incident is identified.

Table 7. Information Source of Disaster

Information Source	Description
Helpdesk	Network failures or critical business applications complained by users / customers.
Personel Back Office (*Network, Data Center*, dll)	Critical business system damage, network failure, security violations, physical threats to IT facilities, infrastructure and buildings (eg fire), personal accidents.
Building Management / Security	Threats to the existence of IT center facilities (fire, bomb threats), and all information received from the emergency center or other local authorities regarding all incidents that may result in the IT center being inaccessible or cannot be used.

It is not enough merely to make contingency strategy plans for information backup, alternative sites, and hardware and software acquisition and replacement; the planning must also include

p-ISSN 0853-7720; e-ISSN 2541-4275, Volume 7, Nomor 2, halaman 321 – 334, Juli 2022
DOI : http://dx.doi.org/10.25105/pdk.v7i2.7082

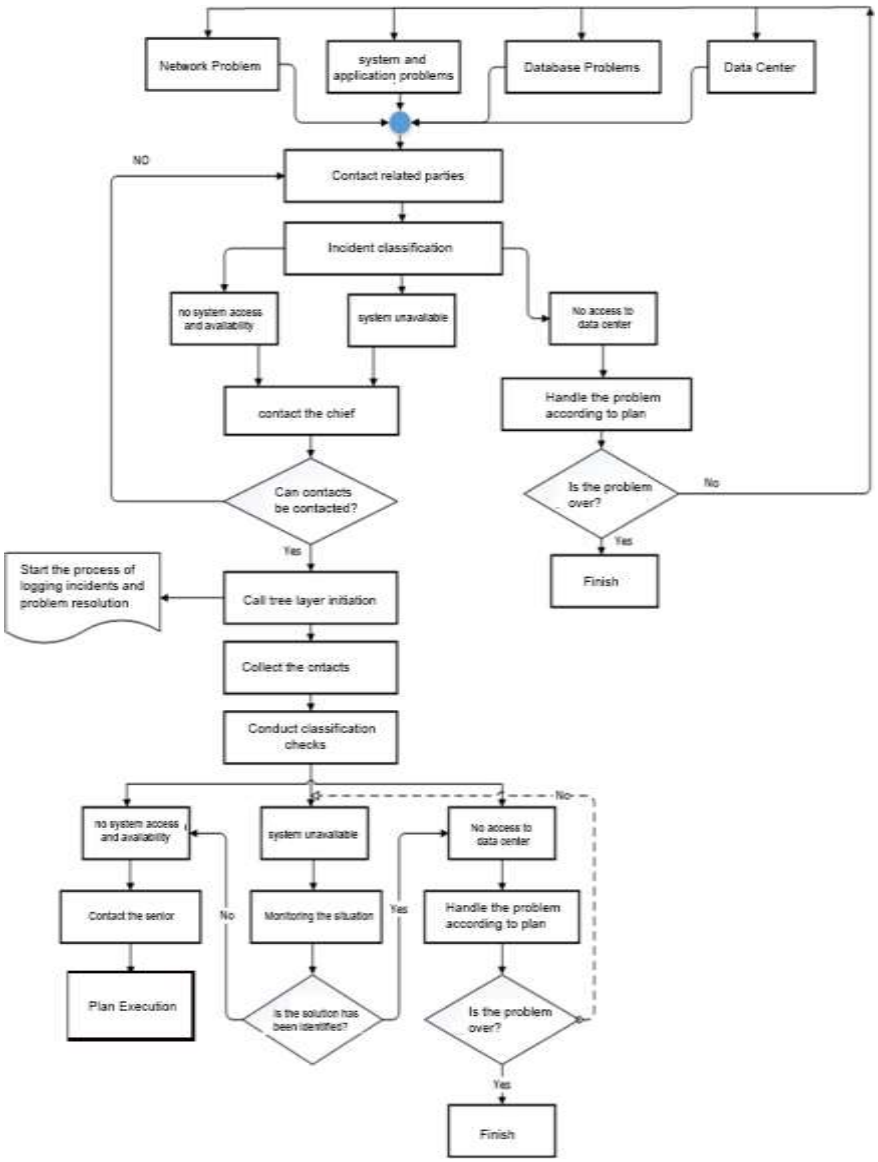
designated teams to implement the various strategies—teams that are trained and ready to respond to the minor or major incident that has triggered implementation of the DRP (Judge, 2013).

Table 8. Classification of Contact Person

Classification of *Contact Person* for each group of problems			
Network	***System & Application***	***Database***	***Data Center***
PI Coordinator	*SI Coordinator*	*DB Coordinator*	*PI Coordinator*
Network Administrator and Network Engineer, Specialist	*System & Application Specialist*	*Database Administrator Specialist*	*System Engineer and System Administrator Specialist*

There is a call tree to execute when a disaster occurs at a later time. Call tree is a hierarchy or tree of people (employees, students etc.) in which each person forwards a message to the next person down the line. The tree is arranged so that a single person can easily forward messages to all people. Graphically depicts the calling responsibilities and the calling order used to contact management, employees, customers, vendors, and other key contacts in the event of an emergency, disaster, or severe outage situation (ENISA, 2015).

p-ISSN 0853-7720; e-ISSN 2541-4275, Volume 7, Nomor 2, halaman 321 – 334, Juli 2022
DOI : http://dx.doi.org/10.25105/pdk.v7i2.7082



Picture 1. Call Tree Disaster Confirmation

5. CONCLUSION

The conclusion and future work based on the results and discussion:

The scope of this research was carried out at UPT-TIK of XYZ University where risk assessment and business impact analysis were carried out to become the basis for the drafting of disaster recovery plan document. Risk assessment was carried out to determine the disaster potential and mitigation that might be occured at the UPT-ICT. Business impact analysis produced critical applications that are managed by UPT-TIK, determined the value of RTO and MTD, and backup strategies for disaster recovery planning, as well as the preparation of a disaster recovery team that contains the responsible parties when a disaster occurs.

p-ISSN 0853-7720; e-ISSN 2541-4275, Volume 7, Nomor 2, halaman 321 – 334, Juli 2022
DOI : http://dx.doi.org/10.25105/pdk.v7i2.7082

6. REFERENCES

Bhatt, G. D., & Grover, V, 2005, *Types of information technology capabilities and their role in competitive advantage: an empirical study* [Electronic version]. Journal of Management Information Systems, 253 - 277.

Bradbury, C, 2008, *Disaster! British Journal of Administrative Management*, 14-16.

Decker, A, 2005, *Disaster recovery: what it means to be prepared* [Electronic version]. DM Review, 44-46.

ENISA, 2015, BCM & Resilience Glossary, Eropa.

Gregory, Peter, CISA, CISSP, 2007, *IT Disaster Recovery Planning for Dummies*, Willey Publishing, Inc, Snedaker Susan, Business Continuity & Disaster Recovery for IT Professionals, Syngress.

Hayes, J, 2005, *Reaping the whirlwind* [Electronic version]. IEEE Review, 29-29.

H. F. Tipton and M. Krause, 2006, *Information Security Management Handbook, Florida USA: Auerbach Publication.*

Judge Herbert B. Dixon Jr, 2013, *Information Technology Disaster Recovery Planning for Court Institutions*. Published in The Judges Journal, Volume 52.

King Ruben [et al.], 2010, *Lessons of Disaster Recovery Learned for Information Systems Management in US Higher Education*, International Journal of Information Systems for Crisis Response and Management (IJISCRAM), Vol. 2. - ISSN: 1937-9390.

L.-K Ronald L. K [et al], 2011, The CISSP Prep Guide—*Mastering the Ten Domains of Computer Security*. Published by John Wiley & Sons, Inc, Canada.

Snedaker Susan, 2007, *Business Continuity & Disaster Recovery for IT Professionals*, Syngress.