JURNAL CAHAYA MANDALIKA

P-ISSN: 2828-495X
E-ISSN: 2721-4796

DESIGN OF DISASTER RECOVERY PLAN BASED ON FRAMEWORK NIST 800-34: CASE STUDY AT PT XYZ OF INDONESIA

Dimas Prihadi Waluya[1], Nico Surantha[2]
[1]Computer Science Department, Binus Graduate Program-Master of Computer Science, Bina Nusantara University, Jakarta, Indonesia
[2]Computer Science Department, Binus Graduate Program-Master of Computer Science, Bina Nusantara University, Jakarta, Indonesia
Email: dimas.waluya@binus.ac.id[1], nico.surantha@binus.ac.id[2]

Keywords:
Disaster Recovery Plan; Nist 800-34; RPO; RTO

ABSTRACT

The purpose of this study to identify Risk assessment in information systems at PT XYZ using the method Octave Allegro and develop Disaster Recovery Plan on the information system at PT XYZ using the NIST 800:34 framework. The downtime on information system that occurred resulted in the disruption of business processes and operations of PT XYZ which currently has 7 main information systems to support the company's business which if not addressed can result in a decrease in user confidence in the company. In this study, a risk assessment will be carried out on information assets owned by PT XYZ using the Octave Allegro method to identify threats to information assets along with the order of threat priority. Then the design of the Disaster Recovery Plan on the information system uses the NIST 800:34 framework containing recovery steps, backup strategies and RPO RTO which are used as priority parameters for information system recovery.

INTRODUCTION

Disaster recovery planning forms to be an important component of any organization to overcome unplanned adversity. To function the successful organization or business model, the structuring of different sectors plays an important role and disaster planning becomes one such core element. Well before the catastrophic event occurs, an organized planned disaster management strategy can overcome the unexpected event and help to recover. In most organization, are equipped with the latest technological fronts but lacks disaster recovery plan management which may often lead to crisis. Even in the current scenario, where a large number of unexpected events are encountered, scanty measures are being implemented to equipped with disaster recovery plan management (Soni, 2020). A disaster recovery plan or any contingency plan would not help in getting profits for business but would definitely help in preventing losses. Especially for companies focus in technology such as marketplaces, a disaster recovery plan is very much needed.

PT XYZ is one of the digital-based trading companies or marketplaces in Indonesia, the results for the last one year period since the operation of PT XYZ's business. There were 58 downtimes in production main service caused by IT system failure or a total of 469 minutes. The downtime that occurred resulted in the disruption of business processes and operations of PT XYZ which currently has 7 main systems, namely the system HRD, Marketplace, Website, Network System,Financial System,Marketing System and Operational System.

Some studies has shown that Disaster Recovery Plan is very important for Business Continuity and Octave Allegro is the appropriate method for conducting risk assessment. Jane, Boonsri,Kim,Kenita (Hom et al., 2020) applied identification risk assessment using Octave method Allegro on the web server and database in institution education. (Hom et al., 2020) Design Disaster Recovery Plan with backup and app recovery using a cloud service, the Designed DRP can protect organization of major system failure, Designed DRP can minimize organizational risk to delay in provision service, DRP can be used for the reliability of system available through testing and simulation. Andrade, Nogueira, Matos, Callou and Maciel (Andrade et al., 2017) Utilization service cloud computing Disaster Recovery as a Service (DRaaS) in backup and enhancement availability of data where Disaster Service Recovery as a service can improve quality and availability effective backup of in terms of resources and cost.

Octave Allegro is a method that uses the Octave approach and is designed to carry out risk assessments on organizational operations with the aim of producing stronger results without the need to explore extensive risk assessment knowledge. This method focuses on information assets in an organization or company in terms of how they are used, where they are stored, carried and processed, and how they are exposed to threats, vulnerabilities, and disruptions. Octave allegro method can be an appropriate risk assessment method for information assets owned by PT XYZ.

The NIST 800-34 framework is a standardization document issued by the National Institute of Standards and Technology (NIST) which aims to provide guidance, recommendations, and considerations in the preparation of an information system contingency plan. NIST 800-34 can be said is a framework that can provide pictures, directions, recommendations and some considerations used in the preparation of contingency plans in information systems. The preparation of an information system contingency plan in NIST 800-34 has a goal that focuses on the steps needed in handling information systems after a disturbance occurs. It is hoped that NIST 800-34 can be the right guide for PT XYZ in designing a disaster recovery plan. NIST 800-34 describes the process of preparing a contingency plan divided into several steps, namely.

a. Develop Continency Planning Policy
b. Conduct Business Impact Analysis
c. Identify Preventive Controls
d. Create Contingency Strategies
e. Develop Contingency Plan
f. Plan Testing, Training, and Exercise.

METHOD

Octave Allegro

The risk assessment process is very important, especially the risks that have a direct impact on PT XYZ's business, both natural and human risks. where this company has a business line in the field of plantation products, so the company needs to manage acceptable risks in the company's operations The risk assessment process based on Octave Allegro begins with identifying threats that have the potential to cause business processes and company operations to stop, especially against critical systems IT (Caralli et al., 2007)

a. Establish risk measurement criteria

   The first activity is to make a qualitative size definition based on the Risk Criteria Worksheet. Risk measurement criteria are used to evaluate the effects or impacts that occur on PT XYZ's information assets in each area and assign priority values.

b. Identify the container of information assets

The Containers are places where information assets are stored, shipped, and processed. In this step, all containers owned by PT XYZ are used to run business operations

c. Identify areas of concern

The activity in this step is the process of identifying areas of concern at PT XYZ using interview and observation techniques with the CEO or Head of IT at PT XYZ in relation to conditions or situations or threats that may occur and can threaten information assets at PT XYZ.

d. Identify threat scenarios

The threat scenario that will be created is the result of the development of the existing threat scenarios in the area of concern. The output of this activity is in the form of detailed information on the area under consideration along with the Mean and Security Requirements that can be carried out by PT XYZ.

e. Identify risks

In the last step, the preparation of risk assessment identification that aims to get a complete risk picture. A threat can have consequences that can have an impact on PT XYZ which can later be used in prioritizing recovery in the preparation of the DRP.

Disaster Recovery Plan Based NIST 800:34

It determines the recovery system for several processes or services that are disrupted after a disaster occurs. Recovery System is an activity of defining a recovery strategy which includes the provision of physical facilities as well as technologies or other supporting systems. The recovery system that has been designed must then be attached to a well documented Disaster Recovery Plan so that it can be easily implemented if a disaster occurs.(Swanson, 2011).

a. Develop Continency Planning Policy

Where at this stage includes the preparation of the main policy elements in making the design of the Disaster Recovery Plan at PT XYZ.

b. Business Impact Analysis (BIA)

Business Impact Analysis (BIA) is an analysis of the company's business processes that are affected by a disaster, where the analysis is carried out by determining which business processes are considered critical and become the main focus in PT XYZ's operational activities and ensuring that these business processes can recover immediately when a disaster occurs.

c. Identify Preventive Controls

The Identify Preventive Controls stage is a stage that aims to reduce or minimize identification at the Business Impact Analysis stage through preventive actions that can prevent the impact of a disaster from occurring and then detect and reduce the impact on the system running at PT XYZ. Where possible cost savings can be achieved.

d. Create Contingency Strategies

The recovery strategy made includes determining alternative locations which also includes determining the system and its infrastructure, then determining the backup-storage method needed by PT XYZ.

e. Develop Contingency Plan

At the Develop Contingency Plan stage or the development of a recovery plan that focuses on several stages to restore existing services at PT XYZ when a disaster occurs such as Supporting Information,Activation Phase and Recovery Phase.

f. Plan Testing, Training, and Exercise

The final stage of the Disaster Recovery Plan system planning is Testing. The Disaster Recovery Plan procedure that is formulated must be tested for feasibility to determine the readiness and impact of the implementation of the Disaster Recovery Plan designed on the running of PT XYZ's business. The purpose of this test or testing aims to determine the suitability and accuracy contained in carrying out the Disaster Recovery Plan procedure when it will be implemented.

RESULTS AND DISCUSSION

List of Assets at PT.XYZ

Based on the list of information technology assets obtained from PT XYZ, the following are assets currently owned by PT XYZ related to the implementation of information technology in supporting current services. Data obtained from interviews with the CEO and Head of IT Network PT XYZ and observations.

Table 1. List of IT Assets at PT XYZ

Category	Sub Category	Asset
Hardware	PC	Asus S500TC
	Laptop	Asus A416JAO
	Switch	Huawei CE6865
	Firewall	Palo Alto 3220
	Server	Dell Power Edge R440
	Load Balancer	Thunder 940 CGN
	Access Point WiFi	Asus RT AC68U
Software	Virtual Server	VMWare ESXI 6.7
	Operating System	Windows Server & Linux
	Application	MS Office, SQL Server
		Internal Application
	Support	Gmail

There are hardware and software categories, hardware in the form of devices that run information systems, applications and PT XYZ databases consisting of PCs, Laptops, Switches, Firewalls, Servers, Load Balancers and Access Points for wifi while the software consists of an operating system that is used on the server side. as well as other devices such as windows server and linux, then some internal applications and SQL server for databases.

Octave Allegro Risk Assessment at PT XYZ

There are several steps that must be taken to carry out a risk analysis according to the working paper from Octave Allegro.

a. Establish Risk Measurement Criteria

There are 5 impact areas that will be evaluated as a result of a risk to PT XYZ's vision, mission and business processes. Risk measurement criteria are used to evaluate the impact of each area as well as to prioritize impacts and qualitative values that can be identified and as a basis for risk assessment of information systems using octave allegro.(Jufri et al., 2017).

Table 2. Reputation Risk Assessment Criteria

Priority	Value	Area of Impact
1	5	Termination of most or all of information systems and applications
2	4	User's Reputation and Trust
3	3	Data Loss
4	2	Material Losses
5	1	Safety

Priorities 1 untill 5 with a weighted value of 1 untill 5 and consists of 5 areas that have an impact on the company starting from a weighted value of 1 for the smallest priority to a weighted value of 5 for the most critical priority.

b. Identifying the Information Asset Container

There are 5 information assets that support PT XYZ business operations then these assets are managed by the IT Division of PT XYZ and the functions of each device in carrying out business operations (Jufri et al., 2017).

Table 3. Information Asset Containers

Devices	Identification of Critical Asset Risk By	Function
1.Server	IT Divison	The device where the application and database run to run the sales platform as well as the entire information system at PT XYZ
2. Switch	IT Divison	Functions to connect all PT XYZ server devices, laptops and PCs to the internet via ISP
3.Firewall	IT Divison	Protecting the internet network and the entire PT XYZ system from cyber security
4. Load Balancer	IT Divison	Optimizing the server to transfer data efficiently, and balancing the workload of PT XYZ's server to avoid server overload
5. Computers	IT Divison	Used by all employees of PT XYZ in running business operations

These assets have their respective functions described in table 3, the function of each asset has its own function or influence on the existing system to run the company business processes.

c. Identifying Areas of Concern

Threats that have or may occur to the company by identifying information asset containers to identify and determine areas of concern that have the potential to threaten the course of information assets at PT XYZ, the Area of concern is expanded to identify threat scenarios and related assets.

Table 4. Table of Areas of Concern

No	Areas of Attention	Related Assets
1	Exploitation of server/database system security loopholes from outside or inside	Server
2	Leaking root or administrator privileges and passwords	Server,Switch,Firewall,PC, Laptop
3.	Damage to server hardware and switches	Server, Switch

4.	Termination of sales website service due to ddos attack	Server
5.	Natural disasters that result in device damage	Server,Switch,Firewall,PC,Laptop

Based on table 4 there are 5 areas or threats that management pays attention to on assets, information systems and business processes of PT XYZ, where if the threat occurs it will have a significant effect on PT XYZ's business operations.

d. Identifying Threat Scenarios

At this stage, the identified areas are then expanded into threat scenarios using a threat tree such as actors, means, motives, outcomes and security for each area of concern.(Jufri et al., 2017).

Table 5. threat scenario identification

No	Areas of Concern	Scenario Threat	
1	Exploit the security system on the server from outside and inside	Actor Mean Motive Outcome Security Reqiurement	Anonymous Gross Force, password cracking Looking for profit, hacking Interruption Update firewall, iptables, Perform data backup
2	Leaking access rights such as root or administrator username and password	Actor Mean Motive Outcome Security Reqiurement	Anonymous, Password scanning and cracking Business competition, For personal benefit Interruption Change passwords regularly Use complex passwords with a combination of letters, numbers and characters
3.	Termination of website service due to ddos attack	Actor Mean Motive Outcome Security Reqiurement	Anonymous Ddos attack Business competition, Get personal benefit Interruption Added anti ddos device

From observations, 3 threats were selected which for the process of identifying threat scenarios with actor, mean, motivation, outcome and security requirements are anticipatory steps that can be taken by PT XYZ to minimize the threat scenario.

e. Identify Risk

The risk identification process at PT XYZ begins by identifying the impact areas and priorities then assigning a quantitative value to the impact value.(Alhawari et al., 2012).

Table 6. Impact Value Identification

Impact Area	Priority	Impact Value		
		Low	Moderate	High

Termination of most or all of information systems and applications	1	5	10	15
User's Reputation and Trust	2	4	8	12

Data Loss	3	3	6	9
Material Losses	4	2	4	6
Safety	5	1	2	3

From observations in table 6 explain the priority areas of impact from 1 untill 5 as well as the impact value with each quantitative value for each impact, either Low, Moderate or High. Then risk Score classification will be carried out and its impact on PT XYZ business operations obtained from the sum of the impact values in each impact area.

Table 7. Classification Impact

Risk Score	Impact
30 – 45	High
16 – 29	Moderate
0 – 15	Low

There are 3 classifications of impacts, namely Low, Moderate and High which have a risk score of 0 untill 15 for Low impact, 16 untill 29 for Moderate impact and 30 untill 45 for High impact. The risk value is obtained by considering the extent of the consequences of the risk impact on various areas of conce.

Table 8. Risk Assesment

No	**Areas of Concern**	**Risk**		
		Affected Area	**Value**	**Score**
1	Exploitation of server/database system security loopholes from outside or inside	Termination of most or all of information systems and applications	High	15
		User's Reputation and Trust	High	12
		Data Loss	High	9
		Material Losses	Low	2
		Safety	Low	1
		Risk Score	**High**	**39**

2	Leaking access rights such as root or administrator	Termination of most or all of information	High	15

	username and password	systems and applications	High	12
		User's Reputation and Trust	High	9
		Data Loss	High	6
		Material Losses	Low	1
		Safety		
		Risk Score	**High**	**42**
3.	Damage to server hardware and switches	Termination of most or all of information systems and applications	High	15
		User's Reputation and Trust	Moderate	8
		Data Loss	High	9
		Material Losses	Moderate	4
		Safety	Low	1
		Risk Score	**High**	**37**
4.	Termination of website service due to ddos attack	Termination of most or all of information systems and applications	Moderate	10
		User's Reputation and Trust	High	12
		Data Loss	Low	3
		Material Losses	Low	2
		Safety	Low	1
		Risk Score	**Moderate**	**28**

5.	Natural disasters that result in device damage	Termination of most or all of information systems and applications	High	12
		User's Reputation and Trust	Moderate	10
		Data Loss	High	9
		Material Losses	High	6
		Safety	High	3
		Risk Score	**High**	**40**

Based on risk identification, observation and referring to the results of interviews with informants, PT XYZ's priority information assets are obtained where 4 threat areas of attention have critical or high risk and 1 area of concern has moderate risk. The five threats can be used as triggers or parameters to use the Disaster Recovery Plan starting with high, moderate and low priority threats.(Aven, 2012)

NIST-Based Disaster Recovery Plan 800:34 PT XYZ

The preparation of a Disaster Recovery Plan for PT XYZ based on the NIST 800:34 framework consists of the following 6 steps:

a. Develop the Contingency Planning Policy Statement

The first stage in developing a contingency plan is to determine a contingency planning policy within the organization. where this arrangement is a form of commitment from the PT XYZ management team to participate in contingency planning.

Table 9. Disaster Recovery Team PT XYZ

No	Roles	Responsibility
1	DRP Lead	Supervise the implementation of PT XYZ's Disaster RecoveryPlan. Responsible for all actions starting from planning to thesuccessful implementation of PT XYZ's disaster recovery
2	Field Engineer	The field team in collaboration with the IT Infrastructure team conducts inspections by monitoring the affected areas, then physically checks the affected equipment including network devices, servers and firewalls and plays a role in monitoring and recording problems that have occurred.
3	Software Engineer	Testing software such as application systems and database systems both on main DC and in DRC, when a disaster occurs Software engineers will swing application systems and databases to devices

		located in DRC. The Software Engineer team also performs regular backups of all data
4	IT Infrastructure	The IT Infrastructure team is tasked with checking physical and logical configurations on every server on the main DC and in the DRC and ensuring that all servers in DRC are ready for use when a disaster occurs so that the data transfer process and system can run properly.
5	Network Engineer	Responsible for managing network systems in the main DC and in DRC and swinging network traffic to DRC so that once a disaster occurs, network traffic can quickly switch links to DRC

b. Business Impact Analysis (BIA) PT XYZ

BIA explains the stages of business impact analysis/platform impact analysis (BIA) which is prepared according to the guidelines from NIST 800-34 (Brar et al., 2015). Its purpose is to identify the business impact if information system services are not available and use the results from the BIA for priority information system recovery. PT. XYZ itself is in the marketplace business line where the sales platform is the fulcrum and source of profit for PT XYZ. From the results of interviews with the CEO and Head of IT Network of PT XYZ, there are 7 main information systems in PT XYZ's business operations and their impacts.

Table 10. BIA

No	Roles	Responsibility
1	HR System	The delay in the employee attendance process
2	Marketplace System	Disruption of the recruitment process, such as CV screening and campus hiring events
3	Website Company System	Users or buyers cannot make purchase transactions
4	Network System (NS)	The seller cannot update the stock of goods
5	Financial System (FS)	Material loss and loss of user trust
6	Marketing System (MS)	Users and potential investors cannot find detailed information about PT XYZ
7	Operational System (OS)	All PT XYZ server devices, PC and Computers cannot connect to the internet

Identified the business impact that will be generated on the 7 main information systems owned by PT XYZ if each of these information systems is disrupted and the impact will disrupt PT XYZ's business operations. Estimated timing. The next stage is determining the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) which will be used in determining the recovery priority consisting of High, Moderate and Low.

Table 11. RPO and RTO

RTO	RPO	Priority
0 - 15 minutes	0 – 30 minutes	High
16 - 30 minutes	31 – 60 minutes	Moderate
31 - 45 minutes	61 – 90 minutes	Low

High priority with RTO 0 untill 15 minutes and RPO 0 untill 30 minutes, Moderate with RTO 16 untill 30 minutes and RPO 31 untill 60 minutes,Low with RTO 31 untill 45 minutes and

RPO 61 untill 90 minutes. From the interviews with CEO and Head of IT Network of PT XYZ, the following are the RTO and RPO of the information system at PT XYZ

Table 12. RPO and RTO System Information

No	System Information	RTO	RPO
1	HR System	45 minutes	90 minutes
2	Marketplace System	5 minutes	15 minutes
3	Website Company System	20 minutes	45 minutes
4	Network System (NS)	5 minutes	15 minutes
5	Financial System (FS)	20 minutes	45 minutes
6	Marketing System (MS)	45 minutes	90 minutes
7	Operational System (OS)	20 minutes	45 minutes

Results show that the marketplace system and internet network system have RTO and RPO with a time of 5 minutes and 15 minutes by referring to table 4.12 the marketplace system and internet network system have the highest recovery priority. Recovery Priority Proposed. Identification of priority for recovery of PT XYZ's information system will be carried out which is classified based on RTO and RPO where the design is expected to be used in determining recovery priorities when disturbances occur in 7 main information systems of PT XYZ

Table 13. Proposed Recovery Priorities

No	Roles	Priority
1	HR System	Low
2	Marketplace System	High
3	Website Company System	Moderate
4	Network System (NS)	High
5	Financial System (FS)	Moderate
6	Marketing System (MS)	Low
7	Operational System (OS)	Moderate

Based on table 13 the results show that the marketplace system and internet network system have a High priority, while the website system, financial system and operational system have a Moderate priority and the HRD system and marketing system have a Low priority.

c. Identify Preventive Controls

Preventive control analysis is carried out by identifying and assessing the types of risks that have been collected.

Table 14. Identify Preventive Control

No	Actions
1	Designing a high availability topology or architecture that allows for a redundancy system that allows if there is damage to one device, other devices can back up
2	Update the firmware and kernel to the latest version

3	Having a redundant network link using several ISPs so that if there is interference at one ISP, the link will move to another ISP

Where of the 7 types of sub-systems that have been identified, 2 systems with High status, 3 systems with Moderate status and 2 systems with Low status, several ways that can be done to minimize or reduce the impact on the system.

d. Create Contingency Strategies

Backup strategy. In order to maintain the continuity of system recovery activities, the information system backup process at PT XYZ must be carried out appropriately. Determination of the backup method based on the information system needs of PT XYZ (Srinivas et al., 2013). In proposing the backup method used, the recovery priority is used based on the proposed recovery priority

Table 15. Backup Strategy

No	System Information	Backup Method
1	HR System	Cold Replication
2	Marketplace System	Hot Replication
3	Website Company System	Hot Replication
4	Network System (NS)	Hot Replication
5	Financial System (FS)	Hot Replication
6	Marketing System (MS)	Cold Replication
7	Operational System (OS)	Hot Replication

Marketplace System, Website System, Internet Network System, Financial System and Operational System are proposed to use the Hot Replication backup method which uses the HA Cluster model which functions to anticipate if a device or OS damage occurs on the host server. While the HRD system and Marketing System are proposed to use the Cold Replication method with RAID which functions to provide tolerance for storage damage physically and logically

Alternate location (DRC). In selecting the alternative site type, PT XYZ's alternative location is based on cost considerations and an assessment of security aspects. So the author proposes a location for backup placement located in DRC which is around the city of Cikarang, West Java. There are several reasons why choosing the DRC location in Cikarang, one of which is the geographical factor, where the main DC and DRC locations are about 40 kilometers and meet the safe distance between the main DC and DRC (35-100 kilometers), in addition to choosing the DRC location. when a power outage or other disaster occurs, the recovery process can run more optimally, so that network latency is not too high. That way, the data backup and restore process can be done without any data loss or zero data loss. In addition, currently in Cikarang, there are already many data centers with minimum qualifications of tier 3 that already exist and are being built, the factor being in the industrial area also makes access to DC easier.

e. Develop Contingency Plan

Supporting information. The recovery plan can be implemented properly. The Disaster Recovery Team that has been formed is expected to play a role and be responsible in accordance with the roles and responsibilities given. Compilation of supporting information in the form of training documents, test documents and maintenance documents that can be used as supporting information in the preparation of the recovery process

Phase activation. This phase is the initial phase that is carried out when an information system service disruption has been detected.(Caralli et al., 2007)

Table 16. Phase Activation

No	Phase Activation
1	DRP Team receives reports of disturbances or threats from either internal or external.
2	DRP The team will conduct a threat analysis and its impact on the company. If it is not an indication of a disaster where the threat does not cause a halt or delay in the company's operations, the threat is given to the relevant unit to be resolved. Meanwhile, if there is an indication of disaster, the DRP team will report the results of the analysis and impact and recommend DRP activation to the DRP Lead.
3	DRP Lead provides status decisions for DRP activation. If not then the threat is given to the related unit to be resolved. If activation is necessary, the DRP Lead will announce a disaster declaration and DRP activation.
4	The DRP Lead will instruct and carry out the activation procedure to the DRP team and instructions for carrying out the Recovery Procedure.
5	DRP Lead provides threat response status reports to other teams

Recovery phase. The recovery phase is carried out when the activation phase has been carried out. Information will be provided to the Disaster Recovery Team to carry out recovery stages that focus on implementing recovery strategies which are expected to repair system damage or disruptions and continue PT XYZ's operational activities.(Caralli et al., 2007)

Table 17. Phase Recovery

No	Phase Recovery
1	DRP Lead performs instructions to run Recovery Procedure
2	The DRP team coordinates with other parties to activate the DRC site.
3	Field Engineer will coordinate with internal to prepare Infrastructure to activate DRC and prepare facilities in alternative locations.
4	DRP team prepares facilities in alternative locations.
5	IT Infrastructure prepares infra in alternative locations.
6	Software Engineer prepares system or application at alternative location.
7	DRP Lead will receive facility readiness status report at alternative location from DRP team
8	DRP team conducts facility testing at alternative locations and reports operational readiness status at alternative locations
9	DRP Lead reports the status of recovery implementation to internal

f. Plan Testing, Training, and Exercise

The next stage is testing and training, the Disaster Recovery Plan that has been designed according to the strategy will be tested and training or drills at PT XYZ are carried out according to the following table:

Table 18. Testing PT.XYZ

NO	Testing	Month
1	Drill Implementation	April
2	Drill Implementation	August
3	Drill Implementation	December

Disaster Recovery Plan testing and training at PT XYZ is carried out 3 times a year, namely in April, August and December every year in the testing and testing carried out, the results of the Disaster Recovery Plan, RPO and RTO testing will be documented as well as filling out the checklist form that has been designed. In addition, after the drill activity, an evaluation will be carried out based on the checklist form. Management of PT XYZ plans to test the Disaster Recovery Plan with test simulations to determine the range of recovery efforts for each information system

Table 19. Form Checklist

No	Phase Activation	State	Note
1	Receive threat reports		
2	Conduct threat and impact analysis with DRP team		
3	DRP Lead provides recommendations for team and internal DRP activation		
4	Provide threat analysis results to related units		
5	Disaster declaration and activation of DRP status		
6	Instructing to run the DRP Procedure		
7	Instructing to run the Recovery Procedure		
8	Reporting the status of DRP implementation		

In table 19 is a checklist form used in the test or simulation of the Disaster Recover Plan that has been designed at PT XYZ

g. Recovery Plan in the DRP

The last stage in the design of the Disaster Recovery Plan is the creation of a recovery plan or recovery strategy where the recovery plan (Florentin et al., 2022). Designed based on the 7 information systems owned by PT XYZ in carrying out its business operations.

Table 20. Recovery Plan

No	System Information	Plan
1	HR System	-Backup data and applications using the RAID method with backup frequency every Monday – Friday -Scheduling server firmware and OS kernel updates -Install and update antivirus
2	Marketplace System	-Backup data and applications using the HA Cluster method which can be used to avoid or minimize disaster and manage planned downtime. Because when a failure occurs at one site, it will not affect the other site, because the cluster has two different locations, namely at the recovery site -Schedule server firmware and OS kernel updates every week -Install and update antivirus and load balancer
3	Website Company System	-Backup data and applications using the HA Cluster method which can be used to avoid or minimize disaster and manage planned downtime. Because when a failure occurs at one site, it will not affect the other site, because the cluster has two different locations, namely at the recovery site. -Schedule server firmware and OS kernel updates every two weeks

-Install and update antivirus and load balancer

		-Anti ddos installation
4	Network System (NS)	-Use HA topology with redundancy system -Use a minimum of 2 – 3 ISPs on each site -Back up the configuration every day -Scheduling switch firmware upgrades every 2 weeks
5	Financial System (FS)	Backup data and applications using the HA Cluster method which can be used to avoid or minimize disaster and manage planned downtime. Because when a failure occurs at one site, it will not affect the other site, because the cluster has two different locations, namely at the recovery site. -Scheduling server firmware and OS kernel updates every 1 month -Install and update antivirus and load balancer
6	Marketing System (MS)	-Backup data and applications using the RAID method with a frequency every Monday - Friday -Scheduling server firmware and OS kernel updates every 1 month -Install and update antivirus
7	Operational System (OS)	-Backup data and applications using the HA Cluster method which can be used to avoid or minimize disaster and manage planned downtime. Because when a failure occurs at one site, it will not affect the other site, because the cluster has two different locations, namely at the recovery site. -Schedule server firmware and OS kernel updates every two weeks -Install and update antivirus and load balancer

CONCLUSION

From the results of the PT XYZ case study, it was found that the designed Disaster Recovery Plan system is expected to eliminate or minimize the main information system and information asset problems causing downtime, where the design results have gone through the stages of integrating needs with the availability of assets and information systems owned by PT XYZ at this time

The results of the risk assessment using the Octave Allegro method at PT XYZ focuses on the information assets owned and results are obtained if the results of the risk assessment on the priority of PT XYZ's information assets have 4 threats in the area of concern having critical or high risk and 1 threat in the attention area having moderate risk

Disaster Recovery Plan design using the NIST 800-34 framework focusing on 7 information systems owned by PT XYZ in running the company's business operations based on RPO and RTO where from 7 types of sub-systems that have been identified 2 sub-systems have High status, namely the marketplace system and internet network system, 3 sub-systems with Moderate status, namely the company website system, financial system, and operational system and 2 sub-systems with Low status, namely the marketing system and HRD system. This research is the design of a recovery plan or recovery strategy that is expected to be implemented on the 7 main systems owned by PT XYZ in carrsying out its business operations.

REFERENCES

Alhawari, S., Karadsheh, L., Talet, A. N., & Mansour, E. (2012). Knowledge-based risk management framework for information technology project. *International Journal of Information Management*, *32*(1), 50–65.

Andrade, E., Nogueira, B., Matos, R., Callou, G., & Maciel, P. (2017). Availability modeling and analysis of a disaster-recovery-as-a-service solution. *Computing*, *99*, 929–954.

Aven, T. (2012). Foundational issues in risk assessment and risk management. *Risk Analysis: An International Journal*, *32*(10), 1647–1656.

Brar, T. P. S., Sharma, D., & Khurmi, S. S. (2015). Disaster recovery and business continuity planning for electronic banking: a comparative study. *ENVISION–International Journal of Commerce and Management*, *9*, 64–71.

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing octave allegro: Improving the information security risk assessment process*. Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst.

Florentin, K. M., Onuki, M., Esteban, M., Valenzuela, V. P., Paterno, M. C., Akpedonu, E., Arcilla, J., & Garciano, L. (2022). Implementing a Pre-disaster Recovery Workshop in Intramuros, Manila, Philippines: lessons for disaster risk assessment, response, and recovery for cultural heritage. *Disasters*, *46*(3), 791–813.

Hom, J., Anong, B., Rii, K. B., Choi, L. K., & Zelina, K. (2020). The Octave Allegro Method in Risk Management Assessment of Educational Institutions. *Aptisi Transactions on Technopreneurship (ATT)*, *2*(2), 167–179.

Jufri, M. T., Hendayun, M., & Suharto, T. (2017). Risk-assessment based academic information System security policy using octave Allegro and ISO 27002. *2017 Second International Conference on Informatics and Computing (ICIC)*, 1–6.

Soni, V. D. (2020). Disaster recovery planning: Untapped success factor in an organization. *Available at SSRN 3628630*.

Srinivas, A., Ramayya, Y. S., & Venkatesh, B. (2013). A study on cloud computing disaster recovery. *International Journal of Innovative Research in Computer and Communication Engineering*, *1*(6), 1380–1389.

Swanson, M. (2011). *Contingency planning guide for federal information systems* (Vol. 800). DIANE Publishing.