Disaster Recovery Plan Level of Readiness in IT-sector

Hadisurya Chandra Kusuma and Yohan Suryanto
University of Indonesia, Margonda Raya Street, Depok, Indonesia

Keywords: Disaster, Pandemic, IT Disaster Recovery Plan.

Abstract: In a pandemic situation like today, the need for mobilization of work is increasing. Plenty of agencies adopt the outsourcing system that makes their networks information vulnerable to threats of attack from outside parties or third parties acting as service providers, the environment, and other physical hazards such as natural disasters or hardware issues, even internal parties themselves. This study measures Disaster Recovery Plan readiness in several agencies in the IT sector in Indonesia. The quantitative methodology in this study is couple with the SPSS Statistical Software, which focuses on calculating the average value as a measure of readiness, classified into two levels, high and low, in each agency divided by their industrial sector. This study shows that the Disaster Recovery Plan Awareness, Disaster Recovery Plan Readiness, and Disaster Recovery Plan Practices, which refer to the ICT DR Service Provision Network, are influenced by three aspects, humans or people, process, and technology or infrastructure. This study's results suggest as the aspects and factors of readiness that should be taken into consideration by an agency in developing and implementing its IT Disaster Recovery Plan.

1 INTRODUCTION

All around the world, businesses are continually increasing their dependency on IT systems for their business processes. The business process that depends on information systems and IT infrastructure directly requires a certain level of availability and recovery, which become the top priorities for unplanned outages and can occur at any time without warning (Rahman, 2014). In a pandemic situation like today, where the need for mobilization of work increases, it is essential for an institution to make early preparations and preventive measures for Disaster Recovery Planning.

Disaster Recovery Planning is one way for an institution to increase awareness and readiness for facing an event that impacts business processes, especially in the IT sector (Shuhaiza & Ibrahim, 2018). Success in the recovery process does not rely solely on documents but three main aspects: human/people, process, and technology/infrastructure to ensure that the recovery process can make the business processes endure during and after a disaster occurs. The approach of this research is to use the models from the previous study and also the existing IT frameworks such as Control Objectives for Information and Related Technology (COBIT) and the International Organization for Standardization (ISO), as well as other literature that supports and provides positive input in analyzing the readiness level of IT Disaster Recovery.

2 LITERATURE REVIEW

2.1 Disaster

Disasters have become an essential issue in the IT sector that can occur without warning, creating a chain of problems for organizations that are not prepared to deal with (Dorasamy, 2010). Disaster can be defined as an event that can occur suddenly, is complex, and results in losses. In Indonesia, the definition of disaster can be seen in Law Number 24 of 2007 about Disaster Management; a disaster is an event or series of events that threaten life and causes losses, both the natural or non-natural factors (BNPB, 2015). Disasters are divided into 2, natural disasters and non-natural disasters. A natural disaster is a series of events caused by nature, such as earthquakes, volcanoes, and floods. In contrast, non-natural disasters are events caused by human factors or occur due to human intervention, such as disease outbreaks

Chandra Kusuma, H. and Suryanto, Y.
Disaster Recovery Plan Level of Readiness in IT-sector.
DOI: 10.5220/0010792000003317
In *Proceedings of the 2nd International Conference on Science, Technology, and Environment (ICoSTE 2020) - Green Technology and Science to Face a New Century*, pages 45-52
ISBN: 978-989-758-545-6

or pandemics. Based on the level, almost every organization worldwide faces the risks that may arise from this level of disaster (Rahman, 2014).

Table 1: Type of Disaster

Type of Disaster	
A	Computer Failure, Corrupted data, Labor Issues, Lost Data, Network Failure, Software Errors
B	Bomb Threat, Bomb Blast, Biological Attack, Disease Outbreaks/Pandemic, Chemical Spill/Attack, Computer Virus, Espionage, Hacking, Human Error, Sabotage, Theft, Terrorism
C	Blackouts, Brownouts, Environmental Hazards, WAN/ISP Failure, Power Surge, Power Grid Failure, Sprinkler System Discharge
D	Earthquakes, Electrical Storms, Fire, Flooding, Hurricanes, Lightning, Tornadoes, Tsunami, Volcano, Wind Storm, Winter Storm

The table above classifies the levels of disasters according to their impact. In a situation like today, a disease outbreak or pandemic is attacking globally, including Indonesia. It affects many sectors, especially the IT sector. The level of mobilization in work increases, which the amount of risk is equal.

2.2 ICT Outsourcing Risk

With the increasing complexity of a modern information system, many organizations adopting an outsourcing system as an option to fulfil their core business activities, especially in the IT sector (Almutairi & Riddle, 2017). However, this is an option that must manage correctly. Because of a significant impact from the perspective of information security, the implemented outsourcing system will be a threat that can cause significant problems to the business as a whole. Several classifications of threats to the ICT outsourcing system (Almutairi & Riddle, 2017) are:

- Threat source, the origin of a threat that can be caused by external, internal, or environmental parties
- Agent, the cause of the threat to occur which could be technical, human, or organizational error
- Types of assets, the asset which is affected by the disaster that occurred

Threat purpose, the threat that arises has a purpose that is intentional or unintentional Type of threat, the threat that occurs can be physical or comes from the environment. The threat can be controlled or cannot be controlled.

Threat impact, the result of the impact and affects one of the three aspects of Information Network Security, namely Confidentiality, Integrity, and Availability.

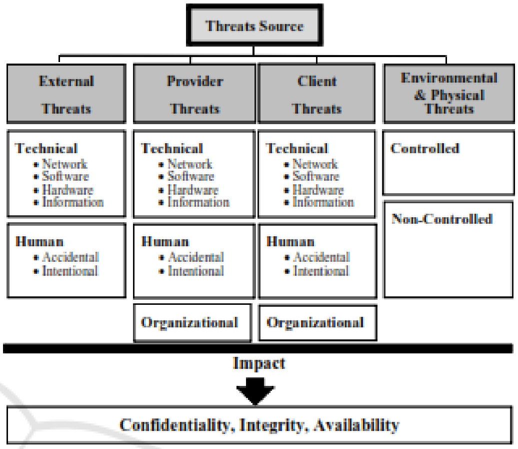


Figure 1. Outsourcing Threat Classification

2.3 Disaster Recovery Planning (DRP)

Disaster Recovery Planning is a comprehensive action procedure taken before, during, and after an event that causes loss of information system resources to respond to emergencies and provide backup operations during an outage and manage the recovery process (Krutz & Vines, 2001).

2.3.1 Disaster Recovery Planning Objectives

The main objective of Disaster Recovery Planning is to provide an organized way to make decisions in the event of a disruptive event and reduce confusion and increase the organization's ability to deal with crises. Of course, when disruptive events occur, the organization will not have the opportunity to create and implement a recovery plan on the spot. Therefore, the amount of planning and testing that can be carried out in advance will determine an organization's ability to deal with disasters. Disaster Recovery Planning has many goals, each of which is very important which includes:

- Protects organizations from major computer service failures
- Reducing the risk for the organization from delays in providing services

- Ensuring the reliability of a system through testing and simulation
- Reducing the slow pace of decision-making required for personnel when a disaster occurs.

2.3.2 Benefits of Disaster Recovery Planning

Disaster Recovery Planning has excellent benefits in reducing the impact of business / organizational losses during a disruption/disaster. Some of the benefits, which is:

- The possibilities for an organization to avoid risks or reduce the impacts of unavoidable disasters
- Improve capabilities in operational business recovery
- Ensuring the system stability in the organization
- Assets and personnel protection
- Reduce disruption and recover quickly when a disaster occurs
- As training materials for new employees.

2.3.3 ICT Disaster Recovery Planning

Following the 5th clause IESO / IEC 24762: 2008, about ICT Disaster Recovery, an ICT Disaster Recovery, whether in-house or using a third party, must follow the instructions described in that clause. If these instructions are followed, it can affect the ability to meet service quality obligations and mitigate the associated risks (International Standart, 2008). These clauses include:

- Environmental stability, the environmental stability needed in a recovery centre to ensure the security and safety of data and personnel
- Asset management, asset management that needs to facilitate recovery from failures and disasters that occur
- The proximity of site, the location of the recovery centre, which is in another area from the company's operational location
- Vendor management, working with relevant service providers in taking the necessary steps.

Outsourcing arrangements, managing the system, and third party personal quality that ensure the safety of business operations.

Information security, ensuring that the organization's information security is not compromised

Activation and deactivation of DRP, the establishment of procedures according to circumstances

- Training and education, the training needed for related personnel who handle DRP to create competent personnel
- Testing on ICT system, periodic system testing to ensure capability and availability when a disaster occurs
- BCP for ICT Disaster Recovery service providers, the ability of service providers to handle internal disaster recovery capabilities before collaborating with organizations
- Documentation and periodic review, all applicable policies and regulations must be documented and reviewed periodically.

2.4 Business Continuity Planning (BCP)

Business Continuity Planning is a method designed to prevent disruptions to business operations and design to protect business processes from failure or disaster, be it natural disasters or human-made non-natural disasters and losses caused due to unavailability of standard business processes (Krutz & Vines, 2001). Business Continuity Planning is a strategy used to reduce the impact of disruptions and allow normal business operations to be resumed. Several essential aspects of the information were seen, which is:

- Local and Wide Area Network and servers
- Telecommunications & data communication links
- Workstations and workspaces
- Applications, software, and data
- Media and records storage
- Staff duties and production processes

2.4.1 Business Continuity Planning Objectives

The purpose of Business Continuity Planning is to prepare, provide, and control the organization's overall capabilities and support the organization's business processes during and after a disaster occurs (International Organization for Standardization, 2009). A BCP can use for a business process within a single business or an entire business process. Also, Business Continuity Planning can use as a long-term recovery stage in conjunction with the Continuity of Operations (COOP), which allows it to use as an additional function of resources and time.

2.4.2 Benefits of Business Continuity Planning

Business Continuity Planning has several benefits that are divide into several points of view (International Organization for Standardization, 2009):

- — A business perspective that protects and enhances the reputation and credibility of the organization
- — A financial point of view that reduces the costs of direct and indirect disruptions
- — An interested party's point of view that takes into account the expectations of the related party
- — An internal point of view that emphasizes increased endurance capabilities during disturbances.

2.4.3 Planning Phase in Bussiness Continuity

Business Continuity Planning uses the concept of the PDCA cycle, Plan (establish), Do (implement and operate), Check (monitor and review), Act (maintain and improve) to periodically implement, maintain and improve the effectiveness of an organization in Business Continuity Planning.

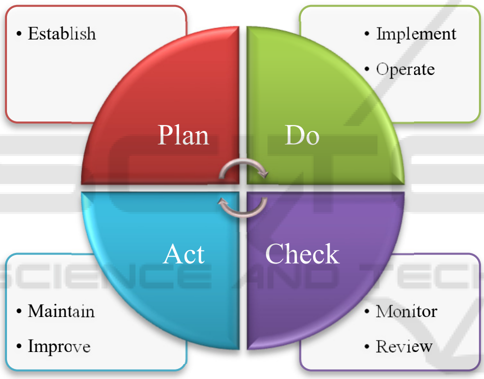


Figure 2. PDCA Concept

Following the PDCA cycle above, this study uses the 6th clause in the BCP. The clause describes the need to establish the strategic objectives and guiding principles of the BCP. Several things in clause six are points for planning:

- Action to address risks and opportunities
- Business Continuity objectives and planning to achieve them
- Planning changes to the business continuity management system

2.5 Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) Differences

BCP and DRP talked about maintaining a business in the face of disruption and returning it to normal. Business Continuity Planning and Disaster Recovery Planning prepare, test, and perform necessary updating actions to protect critical business processes from network and system failures. Of course, these two concepts are so similar that they combine the two into one unit/discussion. However, there are some differences. In essence, BCP is a planning process that will ensure that business functions can survive various emergencies. Meanwhile, DRP, apart from involving preparation for disasters, also discusses procedures to be followed during and after a disaster occurs (Krutz & Vines, 2001).

In short, Disaster Recovery Planning is one of the many plans and analyses required to carry out a complete Business Continuity Plan. The difference is that Disaster Recovery Planning focuses on restoring business operations during and after a disaster occurs, while the Business Continuity Plan focuses on the process of preparing for disaster management (Lachapelle & Hundozi, 2005).

3 RESEARCH METHOD

3.1 Research Approach

The methodology used in a study is critical to link the analytical approach to the results of data analysis so that it can provide answers to research questions and objectives. Therefore, this study uses a quantitative approach and descriptive assessment. The selection of the appropriate methodology and research approach determines the study's quality (Creswell, 2014). Therefore, this research conduct with a 4-stage approach, a preliminary study, the development of research instruments, the actual study, and the last one is the conclusion.

Table 2. Research Approach Phase

Phase	Objectives/Activities	Output
Preliminary Study	Identify and specify the purpose and the focus of the study	Scope and objectives of the research
	Identify the issue	Problem statement
	Literature studies on Disaster Recovery include frameworks, models, awareness and readiness.	Analyzing the aspects and factors of Disaster Recovery Readiness and Awareness
Instrument Development	Design the research approaches instrument which based on Preliminary Study	Develop the online questionnaire survey
Actual Study	Implement an online survey	Collecting survey data
	Analyzing the data using SPSS statistics	Determine the result
	Determine the awareness and readiness measurement levels	Calculating mean and percentage value
Conclusions	Write the final report	Conclusions of the research and the achievement of the objectives, limitations of the study, and future direction

3.2 Development of the Research Instrument

In this study, the research instrument used was a questionnaire distributed online. The questionnaire consists of 3 parts, the first on Disaster Recovery Plan Awareness, the second on Disaster Recovery Plan Readiness, and the third on Disaster Recovery Plan Practices.

In the first part, an assessment is carried out on the awareness of each staff or individual about information security. This assessment identifies the individual or staff's general knowledge of data security and awareness of threats to the data held. In this section, the questions use a nominal scale of "Yes" or "No" as the measurement value.

Then, continue in the second part about Disaster Recovery readiness in an organization. It contains 8 question points that focus on identifying the readiness of an organization in developing Disaster Recovery. Using a nominal scale of 'Yes' or 'No' question as a measure of assessment

Then, the final section consists of 8 question points that identify the implementation of Disaster Recovery in an organization. Using a nominal scale of 'Yes' or 'No' as a measure of assessment

3.3 Target Respondent, Sampling and Distribution

In this study, the sample size consisted of 93 respondents, with the target of this study is individuals who work in the IT department of a company. The number of samples taken is still in the appropriate range in a study based on Roscoe's research (Roscoe, et al., 1975), which states that samples with a range of between 30 and 500 respondents are relevant in a study.

3.4 Hypothesis

In this study, the hypothesis is used as the basis for decision making in calculating the sample at SPSS. The study of related factors referring to the readiness of the IT Disaster Recovery Plan leads to the following hypothesis:

H0: the results from the sample that is studied indicate that the level of Disaster Recovery Plan readiness in the sample of related organizations has a low level

H1: the results from the sample that is studied indicate that the level of Disaster Recovery Plan readiness in the sample of related organizations has a moderate level

4 RESULTS AND DISCUSSION

This study aims to determine the level of readiness and awareness of all agencies regarding the importance of planning and implementing Disaster Recovery Planning in the Information Technology sector as a form of readiness of an agency in facing threats or disasters to maintain reliability. The questionnaires were distributed online and were filled in by 93 respondents who worked as IT staff. The companies that were sampled in this study were companies from various industrial fields, which can be seen in the following table:

Table 3: Industries in The Sample

Industry	Number of Respondents	Percentage
Professional IT Services	29	31.2%
Government and Public Services	16	17.2%
Telecommunication	13	14%
Banking	6	6.5%
Transport and Logistics	5	5.4%
Education	4	4.3%
Energy and Utilities	4	4.3%
E-Commerce	4	4.3%
Others	12	12.8%

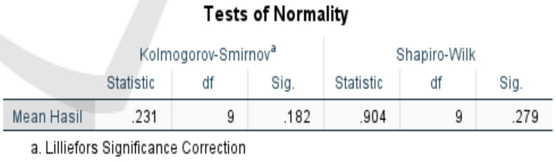
From the sample above, the sample with the most significant number of respondents was companies engaged in IT services with a percentage of 31.2%, followed by respondents who worked for government agencies with a percentage of 17.2%. The research was continued with calculating the average value and testing the standard distribution value, which was then followed by testing the sample t-test value in the SPSS application. The results of the analysis of this study will be able to show the level of organizational readiness for disasters that occur. With the Disaster Recovery Plan, an organization has several planning and preparatory steps for dealing with future disasters.

4.1 Disaster Recovery Plan Awareness

This research begins with an awareness assessment; the assessment is carried out at the level of individual awareness of the security of their information. The findings in this aspect provide an overview of an individual's awareness in maintaining the confidentiality and security of their data. The initial stage begins by determining the average value of each survey question point with the provisions one = Yes, 0 = No, as can be seen in Table 4. To meet the requirements for calculating the t-Test in SPSS, the data must be distributed normally, and the normality value can be seen. In Figure 3. A data can be normally distributed if the Sig. on the normality test > 0.05 (Sig.> 0.05). By using Shapiro-Wilk as a reference basis, the data is normally distributed.

Table 4: IT Disaster Recovery Plan Awareness

Statement	Mean	Level of Awareness
Do you know what to do if your computer is hacked or got infected by a virus?	0.87	Low
Do you frequently access social media using the company's internet network?	0.74	
Do you frequently change your passwords regularly?	0.49	
Have you ever shared passwords and important information with friends virtually?	0.22	
Do you use the same password for various purposes, whether personal or official?	0.59	
If there is an incoming email from an individual or suspicious content, do you delete it immediately?	0.75	
Do you regularly store and back up your important documents on other storage (external Hard Disk or Cloud)?	0.76	
Do you often feel that your devices and stored data are not valuable to be targeted for hacks?	0.52	
Do you obey the Information and Communication Technology (ICT) security regulations that apply to the company?	0.86	



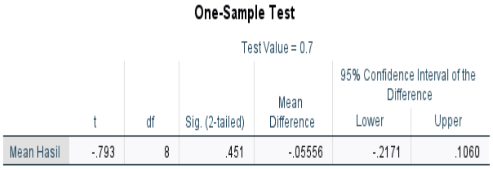
Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Mean Hasil	.231	9	.182	.904	9	.279

a. Lilliefors Significance Correction

Figure 3. IT DRP Awareness Normality Test

The next process is hypothesis testing based on the value of the One-Sample Test analysis on the SPSS application. The reality score of a study has a suggested test consistency score of 0.7 (Boyle, et al., 2015). It can be seen from the analysis of Figure 4 if the results are Sig. (2-tailed) > 0.05, then H0 is accepted, and the results obtained from the Null Hypothesis (H0) are accepted that awareness of the data security of each individual is still low.



One-Sample Test

Test Value = 0.7

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Mean Hasil	-.793	8	.451	-.05556	-.2171	.1060

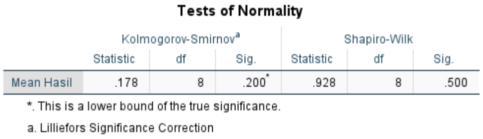
Figure 4. IT DRP Awareness One-Sample Test

4.2 Disaster Recovery Plan Readiness

The next calculation is the readiness for implementing the IT Disaster Recovery Plan. The assessment is carried out by measuring readiness for implementing a Disaster Recovery Plan in an organization. The average calculation uses the provisions of 1 = Yes, and 0 = No, as can be seen in Table 5. It is still using the same calculation method, namely determining the normality value in the data to be continued with the One-Sample Test on SPSS. Figure 5 shows the results of the normality value that has been tested; from these results, it is known that the Sig. > 0.05 so that the data is included in the normal distribution.

Table 5. IT Disaster Recovery Plan Readiness

Statement	Mean	Level of Readiness
Does the company you work for have Disaster Recovery Planning?	0.49	Low
Does Disaster Recovery Planning important for a company?	0.92	
Does the company you work for use third party services/vendors / outsource?	0.68	
Has the company you worked for conducted a trial of Disaster Recovery Planning in the last year?	0.27	
Does the company you work for frequently conduct reviews of Disaster Recovery Planning?	0.29	
Is the Disaster Recovery Planning documented in a straightforward and easy to understand?	0.47	
Has the company you worked for experienced data loss/damage caused by natural / non-natural disasters?	0.20	
Does the company where you work restore the system or other essential services quickly when a disaster occurs?	0.82	



Tests of Normality

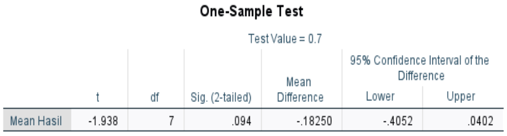
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Mean Hasil	.178	8	.200*	.928	8	.500

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

Figure 5. IT DRP Readiness Normality Test

Next is the calculation of the One-Sample Test to test the research hypothesis. Figure 6 shows the calculation results obtained from the One-Simple Test that was carried out that the Sig. (2-tailed) has a value > 0.05, so H0 is accepted and proves that organizational readiness in the Disaster Recovery Plan is still low.



One-Sample Test

Test Value = 0.7

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
Mean Hasil	-1.938	7	.094	-.18250	-.4052	.0402

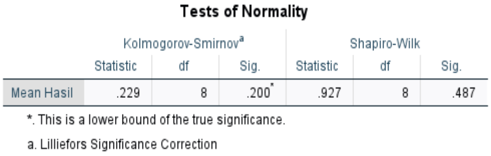
Figure 6. IT DRP Readiness One-Sample Test

4.3 Disaster Recovery Plan Practices

The last part is an assessment of the implementation aspects of the IT Disaster Recovery Plan. The study findings used a nominal scale of 1 = Yes, 0 = No. Measurement of data analysis is preceded by calculating the average of each question point, as shown in table 6, and the normality value will be calculated as a requirement in the analysis calculation, the results of which can be seen in Figure 7. All of these points are influenced by technological factors.

Table 6. IT Disaster Recovery Plan Practices

Statement	Mean	Level of Readiness
Does the company you work for conduct a review of the Disaster Recovery Planning in the event of a cybersecurity threat?	0.56	Low
Does the company you work for have secure and reliable connectivity access for employees who work remotely or work from home (WFH)?	0.87	
Does your company have an IT Support team that manages and supports services to work remotely or work from home (WFH) during peak / off-peak hours?	0.85	
Does the company you work for provide employees who will work remotely or work from home (WFH) about cybersecurity threats?	0.29	
Does the company where you work apply internal and periodic data backup?	0.54	
Does the company you work for have a remote data backup system/remote automatically with encryption security?	0.60	
Does the company you work for have a Disaster Recovery Center (DRC)?	0.48	
Does your company collaborate with service providers in the maintenance and responsibility of data recovery, repair, and replacement?	0.61	



Tests of Normality

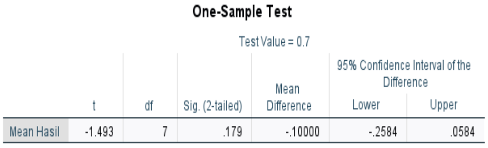
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Mean Hasil	.229	8	.200*	.927	8	.487

*. This is a lower bound of the true significance.

a. Lilliefors Significance Correction

Figure 7. IT DRP Practices Normality Test

The value of the hypothesis test can be seen in Figure 8. The calculation of the One-Sample Test in testing the hypothesis gets the Sig. (2-tailed)> 0.05, so H0 is accepted and proves that the level of implementation of the Disaster Recovery Plan is still low.



One-Sample Test

	Test Value = 0.7					
					95% Confidence Interval of the Difference	
	t	df	Sig. (2-tailed)	Mean Difference	Lower	Upper
Mean Hasil	-1.493	7	.179	-.10000	-.2584	.0584

Figure 8. IT DRP Practices One-Sample Test

5 CONCLUSION

The research conducted in this study resulted in the finding that the level of awareness of individuals and the readiness and implementation of the Disaster Recovery Plan applied to institutions in Indonesia was still low. Lack of infrastructure readiness and documented periodic reviews are one of the causes. Therefore, appropriate budget allocation and reliable staff play an essential role in dealing with disasters. In addition, raising awareness by holding regular training also needs to be provided to all staff as a preventive measure.

In addition, to make all of these things happen, the vital role of management at the top level is needed. So, it requires the involvement of all departments to participate in the planning of Disaster Recovery with the aim that implementation runs smoothly.

The scope of this analysis is expected to provide exposure to awareness, preparedness, and implementation factors and generate mutual interest for the use of new studies in the field of disaster recovery, which can use to develop relevant and comprehensive modules as a guide for institutional preparation.

REFERENCES

Badan Nasional Penanggulangan Bencana, 2015, *Definisi Bencana - BNPB*, https://bnpb.go.id/definisi-bencana, accessed Jun. 02, 2020.

Dorasamy. M, 2010, Disaster Preparedness in Malaysia : An Exploratory Study Multimedia University Faculty of Administrative Science & Policy Studies, WSEAS Transactions on Information Science and Applications, Vol. 7, No. 5, 19–30.

E. Lachapelle, B. Hundozi, 2015, ISO 24762 - Security Techniques Guidelines for Information and Communication Technology Disaster Recovery Service, *When Recognit. Matters.*

G. J. Boyle, D. H. Saklofske, G. Matthews, 2015, *Criteria for Selection and Evaluation of Scales and Measures*, Elsevier Inc.

H. A. Rahman Mohamed, 2014, A Proposed Model for IT Disaster Recovery Plan, *International Journal of Modern Education and Computer Science*, Vol. 6, No. 4, 57–67.

I. Standard, 2008, International Standard ISO / IEC Techniques — Guidelines for Information.

International Organization for Standardization, 2019, ISO 22301:2019 Security and Resilience — Business Continuity Management Systems — Requirements.

J. W. Creswell, 2014, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches 4th edition*, SAGE Publications Inc.

M. Almutairi, S. Riddle, 2017, Security Threat Classification for Outsourced IT Projects, *11th International Conference on Research Challenges in Information, Science (RCIS),* 447–448.

R. Krutz, R. Vines, 2001, *The CISSP Preparation Guide: Mastering the ten domains of Computer Security*.

Shuhaiza Azrin Binti Mohd Kasim, Ibrahim Bin Mohamed, 2018*,* Level of Readiness in IT Disaster Recovery Plan, *Proceedings, 2018 Cyber Resilience Conference (CRC),* 1-4.