*JBTI : Jurnal Bisnis : Teori dan Implementasi*
https://journal.umy.ac.id/index.php/bti/index
*Vol 12, No 1 (2021): April,* **DOI:** https://doi.org/10.18196/jbti.v12i1.10854

# Implementation of Business Continuity Planning Methodology in Making Business Continuity Planning Documents at PT. XYZ

**Ahmad Maulana Fikri[1], Faisal Fachrureza[2], Nadine Octaraisya[3], Nur Amalia Agustyana[4], M. Gilvy Langgawan Putra[5], Dwi Nur Amalia[6]**
[1]*Correspondence Author: 10171001@student.itk.ac.id*
[1,2,3,4,5,6]Kalimantan Institute of Technology, Balikpapan, Indonesia

**I N D E X I N G**
**Keywords:**
*Business Continuity Plan;*
*Business Process;*
*Risk;*
*PT. XYZ;*

**A B S T R A C T**
PT. XYZ is a company engaged in the communication sector. As a company with a national scale, PT. XYZ has various risks, ranging from natural disasters, human disturbances and disruption due to technology. Disruption risks can disrupt the company's operational activities. A business continuity plan document is created to determine the company's steps to minimize damage due to disruption. Making a business continuity plan or BCP starts from the project initiation stage, risk assessment, business impact analysis, mitigation strategy development, plan development, training, testing, auditing. The results obtained from this research are BCP documents used by PT. XYZ in response to a disturbance. With the BCP, PT. XYZ can respond to a disruption that occurs and quickly restore business operations.

**Kata kunci:**
*Rencana Kelanjutan Bisnis;*
*Proses Bisnis;*
*Mempertaruhkan;*
*PT. XYZ;*

**A B S T R A K**
*PT. XYZ merupakan perusahaan yang bergerak di bidang komunikasi. Sebagai perusahaan berskala nasional, PT. XYZ memiliki berbagai risiko, mulai dari bencana alam, gangguan manusia dan gangguan akibat teknologi. Risiko gangguan dapat mengganggu kegiatan operasional perusahaan. Dokumen rencana kelangsungan bisnis dibuat untuk menentukan langkah-langkah perusahaan untuk meminimalkan kerusakan akibat gangguan. Pembuatan rencana kelangsungan bisnis atau BCP dimulai dari tahap inisiasi proyek, penilaian risiko, analisis dampak bisnis, pengembangan strategi mitigasi, pengembangan rencana, pelatihan, pengujian, audit. Hasil yang diperoleh dari penelitian ini adalah dokumen BCP yang digunakan oleh PT. XYZ sebagai respons terhadap gangguan. Dengan adanya BCP, PT. XYZ dapat merespon gangguan yang terjadi dan dengan cepat memulihkan operasi bisnis.*

**Article History**
Received 2021-01-14; Revised 2021-02-03; Accepted 2021-03-06

## INTRODUCTION

According to the PT. XYZ annual report, PT. XYZ is an information and communication company and a complete telecommunications service and network provider in Indonesia. In providing telecommunications services and networks for all Indonesian people, PT. XYZ has several infrastructures such as cables and towers, which are spread in various areas. Of course, multiple risks and disasters can threaten PT. XYZ if not guarded and protected. Suppose there is a risk or disaster in the infrastructure, the business processes at PT. XYZ can be disrupted or even temporarily stopped until conditions recover. Not only that, PT. XYZ's reputation as a service provider can be threatened because of the blocked services. Therefore, a process in business continuity planning is needed by making a Business Continuity Plan or BCP so that business processes can occur even if a disaster occurs. BCP was created to support the vision of PT. XYZ.

Companies need to carry out a business continuity plan or a Business Continuity Plan (BCP) in ensuring business continuity. BCP is necessary to maintain the business processes

owned by the company (Amirullah & Subriadi, 2019). BCP is a company's plan to keep its business continuity (Snedaker S. , 2014). BCP is designed to reduce the negative impact of business disruption caused by internal and external (Asgary & Naini, 2011). Making BCP aims to prevent disruption to normal business activities (Solehudin, 2005). BCP is made with adjustments to the needs and conditions of the company itself (Pertiwi, 2016).

In previous studies, BCP has consistently been implemented for companies and organizations that have critical services. In the case study of PrintGila, which has designed the BCP needed to complete and strengthen the system to become a reliable system (Santoso & Gitarini, 2017). In addition, BCP was also implemented at the Ananda Purwokerto hospital, where SIRUS has been implemented. Still, there are many obstacles in the implementation process, so BCP is needed (Setiawan, Waluyo, & Pambudi, 2019). Industrial companies also need BCP, as in the study by (Wijaya & Widiawan, 2017), which studied the Nail Company in Surabaya. In the government sector, BCP was also designed by (Fajriansah, 2017) and (Zainuri, Nugroho, & Widyawan, 2015) to maintain the continuity of business processes. In this research, a BCP will be designed for PT. XYZ. The design of the BCP will produce a BCP document that defines the possible risks, their impact on business continuity, and the company's steps in mitigating the existing risks. The BCP document will also describe the company's efforts to conduct training, test, and audit the risk mitigation steps.

## LITERATURE REVIEW

### *Business Continuity Planning*

Business Continuity Planning (BCP) is a methodology used to create and validate plans to maintain sustainable business operations before, during, and after disasters or disruptive events. BCP is concerned with managing the operational elements that enable a business to function normally to generate revenue (Snedaker S. , 2014). BCP is a critical component of enterprise risk management initiatives to facilitate business operations under adverse conditions by introducing appropriate resilience strategies, recovery objectives, and business continuity and crisis management plans. In addition, BCP acts as a proactive discipline in identifying vulnerabilities and risks and planning how to mitigate, accept or deploy them in the event of business disruption (Dushie, 2014).

### *Risk Assessment*

Risk assessment is the process of identifying risks or hazards that will occur and analyzing what will happen if these risks arise. Risk assessment is a systematic method to determine whether an organization has an acceptable risk or not. Risk assessment includes risk identification, risk analysis, and risk evaluation (Muhaimin, 2018).

### *Business Impact Analysis*

Business Impact Analysis is a step to understand what business processes are critical in the company. In addition, a business impact analysis can make it easier to understand the impact of disruptions on each running business process. This step will look at the business processes of various existing business functions such as services for consumers, internal operational activities, laws and regulations, and finance. In conducting a business impact analysis assessment, there are several steps taken. The first step is to identify the critical business processes and the most vital business functions in the company. After that, business recovery determines resources and linkages, the impact of each operation in disruption, the

priority of each business process and function, the need for recovery time, and the impact on financial and operational. The result of this stage is a business impact analysis document which is then used together with a risk assessment analysis to produce a mitigation strategy (Snedaker S. , 2007).

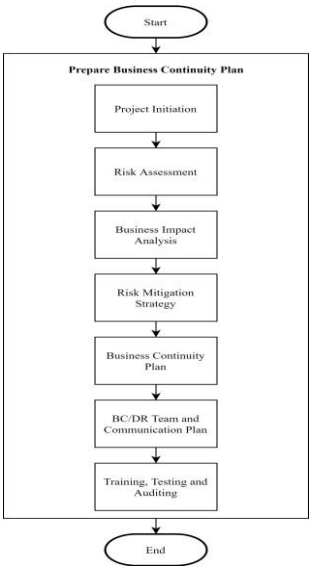
The making of recovery time requirements consists of RPO, RTO, and WRT. RPO stands for Recovery Point Objective, which is the fair amount of data loss from critical business functions. RTO stands for Recovery Tolerable Downtime, which means the time takes to recover business functions from disruptions. WRT is Work Recovery Time which is the time it takes to recover unavailable business functions until they usually run. The time required for each business function varies, depending on where the business function is located. If the business function takes 0 to 12 hours to run normally, then the business function is mission critical. If it takes 13 to 24 hours, the business function is vital. If it takes 1 to 3 days, then the business function is considered necessary, and more than that is deemed minor (Snedaker S. , 2007).

### *Risk Mitigation Strategy*

A risk mitigation strategy is a process plan that develops options to increase opportunities. The risk mitigation strategy is carried out by evaluating the overall risk to reduce the possibility of threats, vulnerabilities, or disruptions that can disrupt business operations, projects, or other business activities (Ahmed, 2017). With a risk mitigation strategy, the entire risk profile of the business is obtained that will help direct the right business decisions. In the risk profile, available what threats might occur, how likely the threats will happen, and how vulnerable the existing system is (Snedaker S. , 2007).

## RESEARCH METHOD

In general, the research was conducted using the Business Continuity Planning method. The following is the method used in the study.




**Picture. 1** Research Methodology

***Project Initiation***

This step analyzed threats and solutions, business needs, functions and technicalities, success criteria, and contributors to PT. XYZ.

***Risk Assessment***

In this step, the risk assessment that might occur at PT. XYZ's complies with the risk criteria was analyzed.

***Business Impact Analysis***

This step would provide an analysis of the business process and its impact on PT. XYZ.

***Risk Mitigation Strategy***

The strategy for preparation of risk mitigation strategies taken for PT XYZ to mitigate risk was provided.

***Business Continuity Plan***

This step prepared a Business Continuity Plan with steps to deal with existing threats.

***BC/DR Team And Communication Plan***

The researchers provided a plan for making BC/DR Team and a Communication plan to arrange for the distribution of responsibilities to the BC/DR team to deal with threats in PT. XYZ.

***Training, Testing & Auditing***

The preparation of training, testing, and auditing for employees of PT XYZ was analyzed to allow employees to overcome threats that may occur.

***Conclusions and suggestions***

At this stage, conclusions and suggestions were drawn based on the research done.

## RESULT AND DISCUSSION

***Project Initiation***

In preparing the design of the BCP document, PT XYZ's needs in each critical area will be prepared in advance. The needs are divided into business needs, functional needs, and technical needs, as follows.

**Table. 1 PT. XYZ Requirement**

| *Critical Area* | *Business Requirements* | *Functional Requirements* | *Technical Requirements* |
|---|---|---|---|
| Consumer | the best connectivity for customers | Providing fixed voice, fixed broadband, IP-TV, and digital services | - Improving business processes regularly<br>- Improving network infrastructure<br>- Compiling Mean time to repair and Meantime to install<br>- Transforming components using optical fiber |

| *Critical Area* | *Business Requirements* | *Functional Requirements* | *Technical Requirements* |
|---|---|---|---|
| Mobile | high mobility for customers | Providing mobile voice, SMS, mobile data services, and mobile digital services | - Having 4G/LTE/HSDPA/3G/EDGE/GPRS technology<br>- Developing electronic money service |
| Enterprise | enterprise service for customers | Providing enterprise connectivity, satellite, and digital platform system services | - Having a high capacity data network with point-to-point and fixed voice connections<br>- Improving data center facilities<br>- Improving cloud services<br>- Developing IoT services |
| Wholesale & International Business | wholesale and international business services for customers | Providing wholesale telecommunication carrier services, tower, infrastructure & network management, and international business | - Using the Indonesia Global Gateway submarine cable (IGG) that connects submarine cables to provide direct broadband connectivity between Europe, Asia, and America<br>- Increasing the number of data centers<br>- Increasing data center capacity<br>- Improving the fiber optic-based backbone network |
| Others | a variety of other services for customers | Providing digital payment solutions, big data & intelligent platforms, digital advertising, music, gaming, and e-commerce services | - Building an ad exchange platform for effective digital advertising<br>- Cooperating with PT. ABC is providing digital music.<br>- Building the XYZ website to facilitate consumer-to-consumer, business-to-consumer, and business-to-business sales |

Table 1 contains the requirements needed to consider a BCP creation. A critical area serves as a scope that needs to be considered for strategy making from BCP. Needs are divided into three namely Business, Functional and Technical Requirements. The three functions are to state the needs from the business, functional and technical side. The needs should be stated so that the BCP can align with company needs and protect critical areas from future threats. The BCP design project can be successful if it meets the criteria stated in Table 2. Success criteria are also required in making the BCP.

**Table. 2 Project Success Criteria**

| *Success Criteria* |
|---|
| PT XYZ has a disaster recovery plan |
| PT XYZ has a crisis management team |
| Carrying out preventive actions in the form of periodic Vulnerability Assessments and Penetration Tests |
| Having a Technology Roadmap by considering new technologies |
| Being able to handle, monitor, and identify all types of attacks in real-time |
| Having recommendations for handling cyber attacks |
| Using information systems to carry out risk management |

***Risk Assessment***

In conducting a risk assessment, the criteria must first be prepared that make this a reference. The following are the criteria for the risk rating.

**Table 3. Risk Rating Criteria**

| **Likelihood of threat event occurrence** | **Likelihood threat event result in adverse impact** | | | | |
|---|---|---|---|---|---|
| | **Very low** | **Low** | **Moderate** | **High** | **Very High** |
| **Very High** | Low | Moderate | High | Very high | Very high |
| **High** | Low | Moderate | Moderate | High | Very high |
| **Moderate** | Low | Low | Moderate | Moderate | High |
| **Low** | Very low | Low | Low | Moderate | Moderate |
| **Very Low** | Very low | Very low | Low | Low | Low |

After determining the risk rating criteria, a risk register is made as a risk assessment at PT XYZ, which is as follows.

**Table. 4 Risk Register**

| **Threat Name** | **Threat source** | **Likelihood** | **Impact** | **Overall Risk Rating** | **Risk Response** |
|---|---|---|---|---|---|
| Flood | External | Moderate | High | Moderate | 1. Risk transfer using asset insurance to anticipate natural disasters and fires<br>2. Coordination for SKKL security<br>3. Preventive & corrective action |
| Lightning | External | Moderate | High | Moderate | |
| Windstorm | External | Moderate | High | Moderate | |
| Earthquake | External | Moderate | High | Moderate | |
| Tsunami | External | Low | High | Moderate | |
| Volcanic eruptions | External | Low | High | Moderate | |
| Plague | External | Very low | Moderate | Low | |
| Fire | External | Moderate | High | Moderate | |
| Drought | External | Very Low | Low | Very Low | |
| Power outage | External | Moderate | High | Moderate | |
| Failure in the continuity of operations | Internal | Moderate | High | Moderate | Reduce risk by providing Integrated Management System (IMS) certification for infrastructure management |
| Cybersecurity threats | Internal | High | Very High | Very High | Prepare recommendations for handling cyber-attacks based on historical incident analysis. |
| Internet service related risks | External | High | High | High | Increase prudence in the preparation of contracts with content provider partners |
| New technology | External | Low | High | Moderate | Prepare a Technology Roadmap by considering future technology and the potential implementation of competitors' technologies. |

| Threat Name | Threat source | Likelihood | Impact | Overall Risk Rating | Risk Response |
|---|---|---|---|---|---|
| Limited operational period of satellite | Internal | Very low | High | Low | Reduce risk by planning to replace satellites that have expired operating life |
| Satellite damage or destruction | Internal | Very Low | High | Low | 1. Satellite operation insurance in the active period<br>2. Manufacturing Insurance and Launching of New Satellites |
| Satellite launch delay or failure | Internal | Very Low | High | Low | 1. Planning for replacement of satellites whose operational period will soon expire<br>2. Satellite operation insurance in an active period. |
| Satellite license revocation | External | Very Low | High | Low | |

Based on the identification and risk assessment carried out (Table 4.), it is found that the risk that has the highest value (very high) is cybersecurity threats. This risk has a high probability (high) and a very high impact (very high). Therefore, PT XYZ responds to this risk to minimize the possibility and implications of the risk.

### *Business Impact Analysis*

Business Impact Analysis is a stage to find out what business processes are critical to the sustainability of PT. XYZ. At this stage, the impact of each business process is also analyzed if these processes experience disruption—business Impact Analysis for PT. XYZ can be seen in the following table.

**Table. 5 Business Impact Analysis**

| *Business Process* | *Customer Impact* | *Financial Impact* | *Reputational Impact* | *Operational Impact* | *Criticality Category* | MTD | RTO | WRT |
|---|---|---|---|---|---|---|---|---|
| Telecommunications and information networks | The customer loses access to communication, and the customer switches to the provider | Decreasing income figures | Decreased reputation due to unstable network | Additional time and salary for network technician | Critical Functions | 11 Hours | 5 Hours | 6 Hours |
| Telecommunication and information technology services | Customers are not satisfied with telecommunication services | Decreasing income figures | Decreased reputation due to suboptimal service | Increased employee salaries but decreased performance | Critical Functions | 10 Hours | 4 Hours | 6 Hours |
| Investment | Investors are not interested in investing because the investment composition is not good | Increased costs for procurement of inappropriate investment goods/technology | Reputation among shareholders decreases due to spending that is not in line with objectives | The investment made cannot streamline the running process | Desirable Functions | 30 Days | 10 Days | 20 Days |

| ***Business Process*** | ***Customer Impact*** | ***Financial Impact*** | ***Reputational Impact*** | ***Operational Impact*** | ***Criticality Category*** | **MTD** | **RTO** | **WRT** |
|---|---|---|---|---|---|---|---|---|
| Payment transaction and money transfer services | Customers have difficulty making transactions if there is no network | High transaction feature maintenance costs | Reputation will decrease if the transaction does not run properly | Additional time and salary for network technician | Essential Functions Vital | 7 Hours | 3 Hours | 4 Hours |
| Other activities and businesses | Customers do not know the company's contribution | There are income and expenses that are not the same | There are no cooperating sponsors | Resources are wasted | Desirable Functions | 5 Days | 2 Days | 3 Days |
| Cooperating with other parties | Customers do not feel the results of cooperation with other parties. | Increased costs for cooperating | Neither party wants to cooperate | Interrupting ongoing projects | Desirable Functions | 30 Hours | 10 Days | 20 Days |

*Risk Mitigation Strategy*

The Risk Mitigation Strategy will define options from various recovery steps that PT can take. XYZ to overcome the risks that occur. The following is a risk mitigation strategy taken based on the consideration of several factors.

**Table. 6 Risk Mitigation Strategy**

| ***Business Process*** | ***Option*** | ***Cost*** | ***Capability*** | ***Effort*** | ***Quality*** | ***Control*** | ***Safety*** | ***Security*** | ***Desirability*** |
|---|---|---|---|---|---|---|---|---|---|
| Telecommunications and information networks | Prepare recommendations for handling cyber-attacks based on historical incident analysis | *Low* | *Meets Requirements* | *Medium* | *Medium* | *High* | *High* | *High* | *High* |
| Telecommunication and information technology services | | | | | | | | | |
| Investment | | | | | | | | | |
| Payment transaction and money transfer services | | | | | | | | | |
| Other activities and businesses | | | | | | | | | |
| Cooperating with other parties | | | | | | | | | |

## *Business Continuity Plan*

The following are the triggers and steps that must be taken in each phase of the Business Continuity Plan. BCP is made based on two departments, namely the IT department and the non-IT department.

**Table. 7 Business Continuity Plan**

| **IT Department** | | |
|---|---|---|
| **Trigger** | **Business Continuity Plan** | **Procedure for Implementation** |
| Cyber-attack threats | Activation of SOP for handling cyber attacks | When there is a disturbance in the form of a cyber threat, the SOP for handling cyberattacks is carried out |
| | Recovery activations | Identify all types of attacks and isolate attacks to reduce their impact |
| | Business Continuity | Inform parties/departments affected by cyber threats |
| | | If the attack cannot be isolated, the IT division will coordinate with related parties to handle cyber threats |
| | | If the attack can be isolated, then the system and data that have been attacked will be repaired |

| | | |
|---|---|---|
| | | Reporting cybersecurity threats to legal authorities |
| | | Perform a malware search |
| | | Perform system and data recovery that has been attacked |
| | Normal Operations | If it is back to normal, then the business process can be run again |
| **Non-IT Department** | | |
| **Trigger** | **Business Continuity Plan** | **Tata Cara Pelaksanaan** |
| Cyber-attack threats | Activation of SOP for handling cyber attacks | When there is a disturbance in the form of a cyber threat, the SOP for handling cyberattacks is carried out |
| | Recovery activations | Inform IT department about received cyber threats |
| | Business Continuity | Informing affected parties of cyber threats |
| | | Waiting for handling from IT department |
| | Normal Operations | If it can be handled, business processes can be rerun normally |

### *BC/DR Team & Communication Plan*

In maintaining business continuity, a structured division of responsibilities is needed in a special team, namely the BC/DR team. Team leaders and members are selected from organizational employees who have the ability, knowledge, and experience to respond to disturbances that occur in the organization. In addition, a spokesperson is also needed so that communication can run smoothly. The following is the BC/DR Team and the Communication Plan executed when a cybersecurity threat occurs at PT XYZ.

**Table. 8 BC/DR Team**

| Title | Role | Phone | Email |
|---|---|---|---|
| Vice President of Corporate Communication | Team Leader | - | - |
| Director of Network & IT Solution | Spokesman | - | - |
| Vice President Infrastructure & | Team Member | - | - |
| Service Performance | Team Member | - | - |
| Executive General Manager Information Technology Division | Team Member | - | - |
| Head of Data Center & Cloud Project | Team Member | - | - |

Responsibilities for each role are as follows:

A. BC/DR Team Leader
- Reviewing the BCP every certain period so that the plan is in line with the company's vision and mission
- Supervising the running of the BCP process
- Facilitating and lead BCP committee meetings
- Deciding on a crisis
- Establish critical indicators of crisis conditions

B. Spokesman
- Explaining the crisis to the communication media

C. BC/DR Team Member
- Recovering assets affected by disruption
- Backing up and restoring data that a cyberattack has attacked

- Documenting the implementation of BC/DR
- Periodically reporting on the development of BC/DR
- Providing recovery recommendations when a cyberattack attacks IT

In the BCP document, it is necessary to determine the communication process so that the information delivery process can run smoothly. The following are recommendations for communication flow in the event of a disturbance/disaster:

1. The communication plan begins when the company experiences a disaster or disruption in business process operations, information technology, and others that can hinder PT XYZ from achieving organizational goals.
2. Departments experiencing disturbances/disasters can independently deal with disturbances/disasters received. If the disturbance/disaster is beyond the control of the affected department, the department can report to the head of the department for assistance.
3. The department head will contact the BC/DR team for initiation and request assistance. The team leader will initiate team activities and hold coordination meetings to address disturbances/disasters.
4. The team leader will assign team members to carry out inspections.
5. Team members will immediately perform recovery according to BCP. Team members will also protect salvageable assets by limiting asset use or temporary deactivation.
6. If a communication media wants to interview the company, the spokesperson will intervene as the only communication channel.
7. If the disturbance/disaster is considered to have a significant impact on operations, temporary suspension of operational activities can be considered. Decision decided by the team leader.
8. Once the disturbance/disaster is under control and the impact can be minimized, the operational transition from recovery to normal can begin. After the operation returns to normal, the BC/DR team will evaluate to assess the performance results and things that need improvement.

***Training Testing & Auditing***

In supporting the success of the business continuity plan that has been designed, training and testing are needed for PT XYZ employees. The training aims to train employees in dealing with cybersecurity threats at PT XYZ. The following is the initiation of a training project that employees will carry out.

**Table. 9 Training Initiation**

| Initiation | Detail |
|---|---|
| Scope | Conducting training to all employees of PT XYZ to be able to take the first step when a cybersecurity threat occurs |
| Objective | • Understanding the role of each individual<br>• Understanding the recommendations for handling cyber threats<br>• Understanding how to back up data correctly<br>• Understanding anti-virus software and how to use it |
| Timeline | Holding training once a year and is mandatory for all employees of PT XYZ |
| Requirement | • Employees of PT XYZ |

| Initiation | Detail |
|---|---|
| | • Cooperating with hackers in Indonesia<br>• Understanding the conditions when the computer is infected with a virus |

The following are training topics that PT XYZ employees need to carry out.

**Table. 10 Training Topics**

| Threat | Training |
|---|---|
| Cyberattacks | Cyber Security Awareness (This training aims to introduce and understand the basics of cybersecurity) |
| | Network Security (This training aims to understand the importance of maintaining security in interacting in cyberspace, such as keeping networks, passwords, and wifi) |
| | Hackers Exposed (This training aims to understand the signs of the emergence of potentially attacking hackers in company technology) |
| | Protect Yourself Online (This training aims to understand how to protect yourself from hackers) |
| | Asset Protection & Safety (This training aims to understand essential protection and security and types of asset security operations) |
| | Emergency Situation (This training aims to understand emergencies in companies and management of mass panic) |
| | Recommendation from Corporate (This training aims to introduce and understand the recommendations for handling cyber threats made by PT XYZ based on historical incident analysis) |
| | Cyber Security Incident Handling and Response (This training aims to understand practices and responses to recommendations made by PT XYZ) |

In ensuring employee understanding of the business continuity plan, a test consists of several stages as follows.

**Table. 11 Training Testing**

| Threat | BC/DR Team | Testing |
|---|---|---|
| Cyberattacks | BC/DR Leader and Member Team | Hacker hacking employee's computer |
| | | Employees are aware of attacks from hackers |
| | | Carry out treatment according to recommendations |
| | | Activate anti-virus application |
| | | If the handling is successful, immediately check the data on the computer |
| | | If the data has been infected with a virus, then do a data backup |
| | | Operation is back to normal |

Before conducting the test, it is necessary to pay attention to several following aspects to run smoothly.

**Table. 12 Testing Audit**

| Threat | Testing | Auditing |
|---|---|---|
| Cyberattacks | Hacker hacking employee's computer | Making sure the company has cooperated with hackers |
| | Employees are aware of attacks from hackers | - |

| Threat | Testing | Auditing |
|---|---|---|
| | Carrying out treatment according to recommendations | • Ensuring handling recommendations are known to all employees<br>• Interviewing each employee regarding the understanding of the recommendations made by the company |
| | Activating anti-virus application | Making sure each employee's computer has an anti-virus application installed |
| | If the handling is successful, immediately check the data on the computer | - |
| | If the data has been infected with a virus, then do a data backup | • Ensuring data backup SOPs are known to all employees<br>• Interviewing with each employee regarding the understanding of SOP data backup |
| | Operation is back to normal | Ensuring that all employees understand the handling of cyber threats |

## CONCLUSION

From the preparation of the BCP, the preparation starts from identifying the risks that have the most significant impact and are likely to be cybersecurity threats. A risk can hinder the running of business processes from various aspects, ranging from the customer, financial, reputation, operational and human. The most appropriate risk mitigation strategy is by considering multiple factors, namely compiling recommendations for handling cyber-attacks based on historical incident analysis. In maintaining business continuity, plans have been prepared to start from SOP activation, recovery, business continuity to normal operations. In addition, the BC / DR team is determined, and training and testing are carried out to allow BCP to run smoothly. The suggestion for further research is to continue improving the sustainability of existing research because the BCP document is a document to develop according to organizational needs and developments in information technology.

## REFERENCES

Ahmed, R. (2017). *Risk Mitigation Strategies in Innovative Projects.* United Kingdom: IntechOpen.

Amirullah, M. I., & Subriadi, A. P. (2019). Evaluation of the Business Continuity Planning Framework at PT. Lotte Chemical Titan Nusantara. *Jurnal SISFO, 8*(2), 87-98.

Asgary, A., & Naini, A. S. (2011). Modelling the Adaptation of Business Continuity Planning by Businesses Using Neural Networks. *Intelligent System in Accounting, Finance, and Management, 18*, 89-104.

Dushie, D. Y. (2014). *Business Continuity Planning: An Empirical Study of Factors that Hinder Effective Disaster Preparedness of Business.* Ghana: Journal of Economics and Sustainable Development.

Fajriansah, C. (2017). *Risk-Based Business Continuity Plan Design at the Sub-Directorate of Information System Development, Directorate of Information Technology and System Development.* Surabaya: ITS Repository.

Muhaimin, M. (2018). Developing Business Continuity Planning (BCP) With A Quantitative Approach Case Study: SIAK-DITJEN Adminduk Mohamina. *Jurnal Sistem Informasi, Teknologi Informasi dan Komputer, 9*(1), 1-11.

Pertiwi, G. P. (2016). *Business Continuity Plan (BCP) Framework for Corporate Information Technology Case Study: PDAM Kota Surabaya.* Surabaya: Institut Teknologi Sepuluh Nopember.

Santoso, G. B., & Gitarini, D. (2017). Design Of Business Continuity Plan Case Study PrintGila. *Jurnal Penelitian dan Karya Ilmiah*, 21-28.

Setiawan, I., Waluyo, R., & Pambudi, W. A. (2019). Business Continuity Plan Design and Disaster Recovery Plan Information Technology and Systems Using ISO 22301. *Jurnal Resti: Rekayasa Sistem dan Teknologi Informasi*, 148-155.

Snedaker, S. (2007). *Business Continuity & Disaster Recovery for IT Professionals.* Burlington: Syngress Publishing, Inc.

Snedaker, S. (2014). *Business Continuity and Disaster Recovery for IT Professionals* (2nd ed.). Elsevier Inc.

Solehudin, U. (2005). *Gunadarma.* Retrieved December 18, 2020, from http://ftp.gunadarma.ac.id

Wijaya, A., & Widiawan, K. (2017). Business Continuity Plan Design for a Nail Company in Surabaya. *Jurnal Titra*.

Zainuri, M., Nugroho, L. E., & Widyawan. (2015). Risk Assessment in Business Continuity Plan Design Case Study: LPSE DIY. *ReTII*.