Regular Article

Ford Lumban Gaol*, Andry and Tokuro Matsuo

Development and implementation of disaster recovery plan in stock exchange industry in Indonesia

https://doi.org/10.1515/eng-2022-0054
received May 16, 2022; accepted July 10, 2022

Abstract: The purpose of this work is to develop and implement a disaster recovery plan (DRP) in stock exchange industry in Indonesia, in order to perform a system recovery in the event of a disaster. To develop a DRP, there are several steps that must be performed as a risk analysis to determine how much risk the company would receive when a disaster occurs, business impact analysis to identify critical business units and necessary resources for the recovery process to run smoothly, to identify recovery strategies to be used as a backup method and recovery site, the recovery procedure that needs to be done in order to make the recovery process run properly, testing and review, and documentation of the DRP. Based on the results of tests that have been done, the development of DRPs can be implemented at stock Exchange industry in Indonesia. With the DRP, the company is expected to have a plan to prepare for and recover resources and information systems in order to be able to walk back in the event of a disaster in order to minimize losses to the company.

Keywords: disaster recovery plan, business impact analysis, risk analysis, recovery procedure, documentation

1 Introduction

Information system has been an important part of a company because the entire business processes use computer systems. To support the business services, the company has the IT infrastructure such as data centers that connected with regulator (Indonesia stock exchange) so that remote trading system used for trading can run [23]. Remote trading system itself is trading remotely using host to host order routing interface system where the Indonesian stock exchange provides an application interface for securities firms. As mentioned, the company brokerage office information system will connect to this application with the IDX trading system [4].

As mentioned in ref. [13], transactions in the securities companies occur in matter of seconds because when the customer orders buy or sell, the order must be entered into the system as soon as possible. If the system is experiencing interference and cannot be used, then the company may suffer losses. Availability of system needs to be maintained to ensure that there is no downtime on the system. As mentioned in ref. [18], there are various things that can enable the occurrence of problem that caused the system to be not usable, such as hardware failure, error in the system, human error, natural disasters such as floods and fires, and terrorist.

2 Statement of problem

Indonesia stock exchange as regulator capital market in Indonesia issued a regulation that every securities company should have a business continuity plan (BCP). As mentioned in refs. [5,6], to fulfill the required obligations as a securities company, the company made plans to develop disaster recovery plan (DRP). As mentioned in ref. [9], the company also realized that in addition to fulfilling the obligations of the regulator, DRP also improves the availability of system where the company can restore the system quickly so that business operations can be run back when disaster happens. As mentioned in ref. [7], developing a DRP is not easy and there are several steps that need to carried out.

* **Corresponding author: Ford Lumban Gaol,** Computer Science Department, Binus University, Jakarta, Indonesia, e-mail: fgaol@binus.edu
Andry: Master of Information System, Binus University, Jakarta, Indonesia, e-mail: andry.andry@binus.ac.id
Tokuro Matsuo: Research Center for Service Science and Artificial Intelligence, Advanced Institute of Industrial Technology, Tokyo, Japan, e-mail: matsuo@aiit.ac.jp

3 Methodology

The methodology used in this study, as mentioned by refs [1,25], was to make the following the BCP guidelines for the Exchange Member that has been given by the regulator where the guidelines use the reference from BS 25999-1: 2006. There are several steps that need to be carried out to develop a DRP [24]. As mentioned in refs [11,15], the first step of development is to create an organizational structure of resources who will be responsible for the implementation of the DRP and allocating existing resources and determine the duties and responsibilities of each. The next is a risk analysis to determine how much risk the company would receive when a disaster occurs. As also mentioned in ref. [12], the next stage is business impact analysis (BIA) for identifying the critical business units and the resources necessary for the recovery process to run smoothly. As mentioned in ref. [17], the next stage is recovery strategies that are used as methods of backup and recovery locations are used, recovery procedures that need to be followed during a recovery, testing, and review of the DRP were made and documentation of the DRP development results are done.

3.1 Project initiation

As mentioned in ref. [19], the first step in the development of DRP is to make the organizational structure of resources who will be responsible for running the DRP and allocating duties and responsibilities to resources of each team. The organizational structure created can be divided as follows:

- Business continuity management (BCM) steering committee
- Disaster recovery team
- Emergency response team
- Crisis operations team
- Crisis recovery team
- Compliance team

As mentioned in ref. [20], each team consists of a team leader and team members. Executive management is responsible for determining the team leader and team members. Team leader is responsible for coordinating the team members to work in accordance with the responsibilities that have been determined.

3.2 Risk analysis

Risk analysis is a process for identifying threats and measuring the level of risk that is acceptable to the company. As mentioned in ref. [15], the method used in risk analysis used references from ref. [17], guide for conducting risk assessments. As mentioned in ref. [17], the early step of risk analysis begins by identifying threats and vulnerabilities in the company information system that can be exploited by threat. Threats can be grouped into unauthorized access (hackers, etc.), structural issues (hardware failure, software malfunction, network failure, etc.), and environmental issues (fire, flood, earthquake, terrorist/bombing, power outage, etc.) [26].

As mentioned in ref. [14], threats and weaknesses can be identified from the system information specification that was gathered from various information such as questionnaires and documentation. The next step is to determine the likelihood. Likelihood is the analysis of the likelihood rating that can be explained from very low, low, moderate, high, or very high. The next step is to determine impact rating of the threat that could cause the downtime of the information system and thereby loss for the company. Impact rating can be explained from very low, low, moderate, high, or very high depending on how big the impact on the company is. The last step is to determine the level of risk. As mentioned in ref. [21], the level of risk can be obtained by multiplying the value of likelihood rating and impact rating as shown in Table 1 below.

Table 1: Risk level matrix [21]

Likelihood	Level of impact				
	Very low	**Low**	**Moderate**	**High**	**Very high**
Very high	Very low	Low	Moderate	High	Very high
High	Very low	Low	Moderate	High	Very high
Moderate	Very low	Low	Moderate	Moderate	High
Low	Very low	Low	Low	Low	Moderate
Very low	Very low	Very low	Very low	Low	Low

3.3 BIA

As mentioned in ref. [2], BIA is a business analysis that measures the impact of a disaster on the company to define the business processes that are considered critical and the main focus of the company's business continuity activities. The method used in the BIA is as mentioned in ref. [8], using references from ref. [16], contingency planning guide for Federal Information Systems. As mentioned in ref. [22], there are 3 steps involved in BIA:

1. Identify critical business processes at work unit

   System information in a company can be very complex and often support multiple business processes. Each work unit has a different system to run business operations. In order to better understand the impact of system outages or disruptions in the company, we must identify critical business processes and processes that depend on information technology. To identify critical enterprise work units, we need to analyze the company business processes in order to determine the work unit that uses the system for every day operations so that when the system encountered a problem and cannot be used then the business operations will be halted.
2. Identify required resources

   Restoration requires an analysis of the resources needed in order to continue the business process as quickly as possible. We need to identify the critical resources to analyze the company's business processes to determine the information systems used by the critical work unit in running the business operations.
3. Identify system information priority recovery

   Based on the results of the previous process identification, priority recovery can be determined by considering the critical business processes that are directly related to the company's information system. Results of identification will get priority order recovery system used in the disaster recovery process.

3.4 Recovery strategy

Recovery strategy is needed to reduce the risks arising from the interruption of information systems. Recovery strategies include backup method that will be used, and location alternatives including systems and infrastructure.

3.5 Recovery procedures

As reported in refs. [3,5], recovery procedure is a set of procedures established to regulate the procedures performed by the employee in carrying out the DRP when a disaster occurs until the restoration of the company business operations. Recovery procedure is based on reference guidelines of BCP exchange members and adapted to the company's standard operating procedure (SOP) [10].

3.6 Testing and review

After all the DRP development process is completed, testing needs to be done to ensure effective implementation of DRP that has been created to work well in a state of disaster. The testing process is carried out by making a simulation. Simulations will be conducted on a Saturday, wherein the disaster scenario has occurred at the central office so that the system in the data center cannot be used. The testing process will also be assisted by external reviewers who will oversee the running of test simulations of DRP the company and report the results of testing the DRP after completion.

3.7 Documentation

Results of DRP development will be documented into a report that will be used as a guide in implementing the DRP.

4 Result

The results obtained from this study are DRP that includes a DRP organizational structure, risk analysis, BIA, recovery strategies, recovery procedures, review testing and documentation required in the company to recover when disaster strikes.

4.1 Project initiation

In the first step, we need to ask approval from management before starting the project because the management is responsible and involved in the process of developing DRP. Next we need to establish an organizational structure to support the implementation of DRP in order for the recovery to be carried out effectively. The organizational structure is described as shown in Figure 1:

- BCM steering committee is a committee/board of directors consisting of executive management that make strategic decisions related to business continuity planning.

- Disaster recovery team acts as the main coordinator of all activities of the DRP which coordinates with all other teams to operate DRP.
- Emergency response team to act as a coordinator in the initial response at the time of the disaster, which is responsible for the evacuation of resources for human safety and the protection of critical company assets.
- Crisis operations team acts as a coordinator in the recovery of the company operational processes performed by each unit of work.
- Crisis recovery team acts as a coordinator in the process of recovery systems and infrastructure that will be used temporarily when a disaster occurs.
- Compliance team acts as the main coordinator in monitoring the compliance function of company policy and regulations in the process of recovery of business processes.

The person who initiates this recovery operation is chosen from the BCP steering committee, who will send instructions to the lower level individuals detailing the steps to be performed.

4.2 Risk analysis

The next step is risk analysis. Risk analysis is a process that begins with the identification of threat, vulnerability, likelihood, impact, and level of risk. Threats and vulnerabilities of information systems are obtained from data collected from a wide variety of information such as questionnaires and documentation. Threats and vulnerabilities are listed in Table 2 below:

Likelihood rating obtained from interviews and documentation: Results of the interviews will be analyzed using the mode method to find the data most frequently occurring or has the greatest frequency. The Impact result will be obtained from interviews. Results of the interviews will be analyzed using the mode method to find the data most frequently occurring or has the greatest frequency

Results of data collection likelihood and impact rating that has been collected are listed in Table 3 below.

From Table 3, it can be seen that for earthquakes and terrorist/bombing, threats have a low risk level which means that if the threat occurs, it can provide a limited adverse effect on the operations of the company, the assets of the company, individual, or other organizations. Hackers' threat has moderate risk level which means that if the threat occurs, it can give a serious adverse effect on the company's operations, assets of the company, individual, or other organizations. Software malfunction, network failure, hardware failure, fires, floods, and power outages have high risk level which means that if the threat occurs, it can give a severe adverse effect on the company's operations, asset, individuals, or other organization.

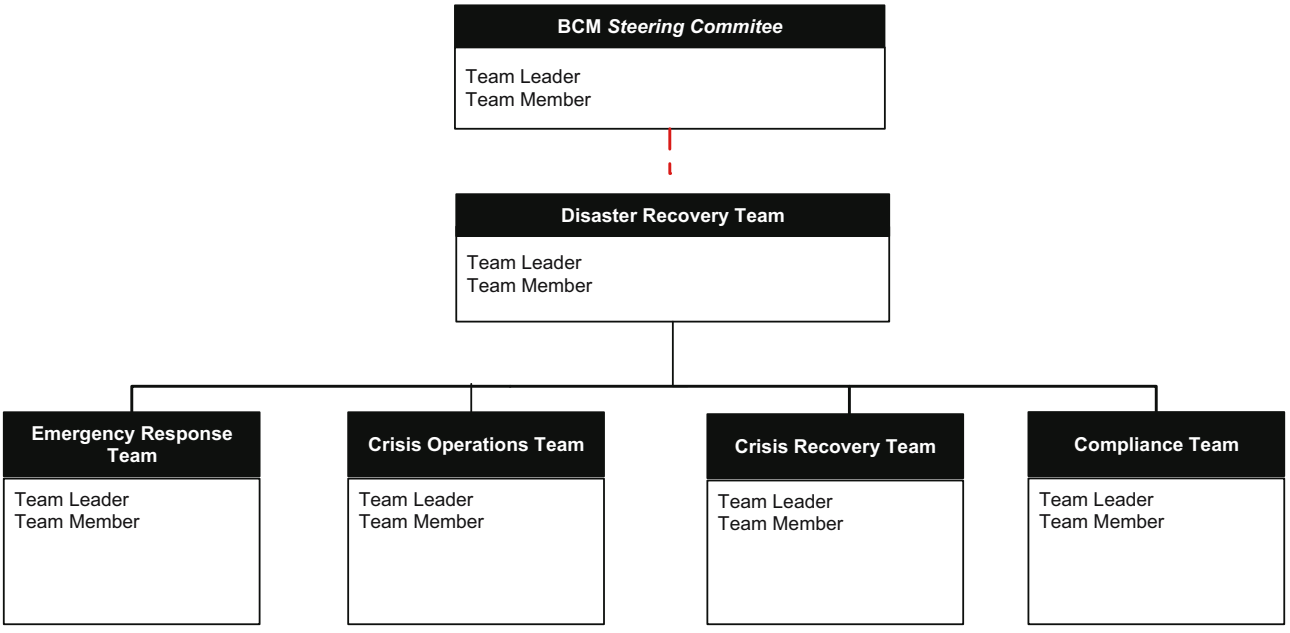

Figure 1: Organizational Structure of DRP.

Table 2: Threats and vulnerabilities identification

Threat	Vulnerability
Hacker	Data manipulation and theft can result in the corporate data losing their integrity and becoming corrupted
Software malfunction	Software malfunction can lead to application becoming corrupted or data loss
Network failure	Failure in network can cause disorders in systems and business operations
Hardware failure	Hardware failure can create interference on the entire system
Earthquake	Earthquake causes damage to the building making the office inaccessible and causing damage to the data center
Fire	Fire makes the main office inaccessible
Flood	Flood makes the main office inaccessible
Terrorists/bombing	Terrorists/bombing cause damage to the main office building making the office inaccessible
Power outage	Power outage makes system non-usable and stalls the business operations stalled

Table 3: Risk level

No.	Threat	Likelihood rating	Impact rating	Risk rating
1.	Hacker	Moderate	Moderate	Moderate
2.	Software malfunction	High	High	High
3.	Network failure	High	High	High
4.	Hardware failure	Moderate	High	High
5.	Earthquake	Very low	Very high	Low
6.	Fire	Moderate	High	High
7.	Flood	High	High	High
8.	Terrorist/ bombing	Very low	High	Low
9.	Power outage	High	High	High

For the threat of hacker, we implemented the Use Multi-Factor Authentication and implemented the Password Manager

We implemented continuous and effective testing as well as having a solid software execution plan and pre-road-mapping plans can help your team go a long way in effective software development on the risk reduction on software malfunction.

Failure in networking can occur in routers and switches, as well as services such as DHCP and DNS servers, and everything else that keeps data moving on your network. Data cables and power supplies to the data center are further examples where resource failures can occur. Preventing such consequences can take numerous sorts. The first and most evident requirement is long-term power production capability. When electricity is off, most data centers feature diesel generators that can run for extended periods of time with little impact on the business. There is also battery backup linked to an inverter to function as a buffer between when the main power goes off and when the generator powers up.

Hardware failure can occur when components of your IT infrastructure cease to function. Hardware failure can occur for a variety of causes, including power grid voltage spikes, water damage, or electrical component failure due to age or a lack of maintenance. These can have a particularly catastrophic impact on operations if not properly planned for. The prevention includes maintenance of fans, ducts, and filters on a regular basis on all the servers and rack-mounted equipment. Dirt will eventually clog the airflow of any equipment that has a fan (or numerous fans) installed.

To explore more we apply on measurement on earthquake risk using engineering risk analysis. Experts can determine the likelihood of each cause of failure, the likelihood of earthquake that might harm the facilities, and the likelihood that an earthquake will leave the facility inoperable for a specific period of time following the earthquake. The same calculation may be conducted if specific adjustments are implemented, such as anchoring equipment, installing emergency generators, on-site water supplies, and so on. With as-is and what-if risk estimations, one may make more educated judgments regarding the costs and advantages of remediation. Contingency plans can be designed for situations that cannot be remedied cost-effectively.

There are several things you can do to avoid a fire – in some circumstances, fire prevention is more effective than any fire protection device. It is advised that you use the most recent edition of NFPA 75: Standard for Fire Protection of Information Technology Equipment from the National Fire Protection Association.

In addition, we can use the following fire prevention strategies:

- Store combustible goods away from the computer room – storing combustible materials in the computer room increases the likelihood and spread of fire. Keep supplies to a minimum in the area and keep boxes, packing, and manuals elsewhere.

- Check power cords – frayed or broken power lines provide a fire hazard since a spark might readily ignite the area. We need to check for damage and have repairs done as soon as possible.
- Train staff and post fire emergency plans – making sure the personnel understand how to react to a fire (whether that means using a fire extinguisher properly or promptly evacuating to safety) may save lives and help avoid more damage.
- Schedule frequent fire protection system inspections – the life safety and fire protection systems are only effective if they are in good working condition. Schedule frequent inspections with a competent fire prevention firm in certain area, such as state systems. They can check that the equipment is not only operational, but also that it complies with all local and state fire regulations.

Flood: water damage in the server room and data center will have serious consequences. Not all water damage in a data center, server room, manufacturing facility, or warehouse must be severe. Water penetration often causes merely a short-circuit. Larger floods will probably cause significant damage to the computer center. We recommend using a water leak detection system with sensors and alarm servers. Water leaking may be detected early with the use of a water sensor or the new water-detection chain. The sensor probe remote monitoring equipment will notify IT employees of accidents in the computing center/server room/production area by email, SMS (via gateway), or SNMP trap to network monitoring system.

Terrorist/bombing: we maintain regular touch with the government entity that takes up security measures to safeguard persons and organizations that might become targets of terrorist/bombing attacks. This lowers the likelihood of a terrorist assault. We maintain regular touch with the government entity that takes security measures to safeguard persons and organizations that might become targets of terrorist/bombing attacks. This lowers the likelihood of a terrorist assault.

There are three ways to protect data during a power outage such as power outage, power spikes, power outages and brownouts. Installing an uninterruptible power supply (UPS) is an effective method of protecting data against brownouts and unexpected power outages. While the user saves active data, the system keeps the computer functioning for a few minutes longer. The user may then securely shut down the equipment without causing damage to the devices or losing data. The UPS is often used as a battery backup solution for a computer.

Even if a generator is installed, a UPS is strongly recommended to avoid the short power loss during which data is lost and equipment is harmed until the generator kicks in. With power outages and load shedding occurring on a weekly basis, a comprehensive strategy must be put in place to limit the harm caused.

4.3 BIA

4.3.1 Identify critical business processes at work unit

In this step, we will identify company business processes by analyzing the company business processes that use information systems for daily operations in order to determine the critical business processes that need to be prioritized in the event of disaster recovery. The detailed result of this step is shown in Table 4.

Table 4: Critical business processes

Work unit	Critical business processes
Sales	Acceptance and cancellation of customer orders
Risk management	Determination of customer trading limit
	Verification orders and other instructions from the customer
Finance & accounting	Recording of all financial transactions
	Daily reconciliation between general ledger and security ledger
	Reconciliation Modal Kerja Bersih Diperhitungkan at the end of day
Settlement	Settlement of securities transactions
	Acceptance, delivery, and storage of funds related to securities
	Maintenance of records and books include accounts of securities companies, securities ledger, ledger funds, and sub-ledger transactions
Compliance	Supervision of compliance of the business operations with the policies and SOPs, and regulations
	Handling customer complaints and help to solve it.
ICT	Handling problems that occur on the system and network
	Maintenance of databases and applications
	Handling system connection with the Indonesia stock exchange

4.3.2 Identify resources required

In this step, we need to identify the critical resources for running the business operations of the company to be prioritized to do recovery when disaster strikes. Identification process was carried out by analyzing the company's business processes to determine the information systems used by the critical work unit in running the company operations.

The detailed results of this step are shown in Table 5.

Base on Table 5, the platform that we used is Hewlett Packard Enterprise (HPE) rack mounted servers, notably the HPE ProLiant DL360 Gen9 type, was used as server hardware.

HPE FlexFabric (FF) switches, the HPE FF 5930, and HPE FF 5700 were utilized as network switches.

The Red Hat OpenStack Platform controller, computer, and director nodes will be hosted on the HPE ProLiant DL360 Gen9 1U rack mount server.

Specifications:

1. Intel Xeon E5-2600 v3 processor family; Intel Xeon E5-2600 v4 processor family
2. Core processor: 18
3. 1.5TB memory
4. Dynamic Smart Array B140i storage controller

Based on Table 5, the remote trading system was the critical systems and applications that provide impact to sales and risk management. The remote trading system also provides support and critical servicesthat able to make buying and selling shares transaction.

Sales is also dependable on the systems and applications data feed system and JONEC System. Both the systems are connected to the Indonesia stock exchange system to receive market information data. File server is the complex and critical server that handled sales, settlement, finance and accounting, risk management, ICT, and compliance. The file server is used to save files and company's important data. Back office system is critical to manage stock transactions, customer funds, customer data, etc. The back office system is the system that relates heavily with the unit system on settlement, finance and accounting, as well as risk management.

4.3.3 Identifying priority system recovery information

Priority recovery can be made by considering the critical business processes that are directly related to the company's information system that has been identified in Section 4.3.1. The critical business processes will be identified based on:

1. Maximum tolerable downtime (MTD) is the maximum amount of time that a business process can be inoperable before threatening the organization's survival.
2. Recovery time objective (RTO) refers to the amount of time and the service level that must elapse between

Table 5: Critical resource

Systems and applications	Work unit	Platform/OS/Version	Explanation
Remote trading system	• Sales • Risk management	HP DL360/Windows Server 2008 Standard/Service Pack 2	System to make buying and selling shares transaction
Data feed system	• Sales	HP DL360/Windows Server 2008 Standard/Service Pack 2	Systems connected to the Indonesia stock exchange system to receive market information data
JONEC system	• Sales • ICT	HP DL360/Windows Server 2008 Standard/Service Pack 2	Systems connected to the Indonesia stock exchange system to send and receive stock transaction
Back office system	• Settlement • Finance and accounting • Risk management	HP DL360/Windows Server 2008 Standard/Service Pack 2	System to manage stock transactions, customer funds, customer data, etc.
File Server	• Sales • Settlement • Finance and accounting • Risk management • ICT • Compliance	HP DL360/Windows Server 2008 Standard/Service Pack 2	The server is used to save files and companies important data

the occurrence of a disaster and the restoration of a business process. This is done in order to avoid the unacceptable effects that are connected with a disruption in continuity.

3. Recovery point objective (RPO) is the maximum quantity of data – measured in time – that can be lost following a recovery from a disaster, failure, or similar incident before data loss exceeds an organization's tolerable threshold.

Based on the identification result shown in Table 6, priority order recovery system will be used in the disaster recovery process.

4.4 Recovery strategies

4.4.1 Alternate recovery location

A disaster recovery center (DRC) is a building or mobile office where people can go to get information about disaster aid programs or ask questions about the disaster. The company makes DRC as an alternative recovery data center in the event of disaster. DRC is used by companies including reciprocal site that is an alternative facility provided by regulator for each security company one rack server as a support to the capital market industry.

DRC facility used a type of warm site facility wherein the DRC was already provided with hardware, network connections, and electrical power that can be used in the event of a disaster at the primary location. Systems and applications are already installed on the device in the DRC and restoration of the database must be done before the system can be used. DRC facility can only be used for recovery in the event of disaster that caused main office to be unusable.

The distance between DRC and main data center is approximately 60 km to connect the network between the two data centers using MPLS network with bandwidth of 1 Mbps, while Internet network in DRC uses the network with bandwidth of 5 Mbps. Besides DRC, company also has facilities for alternative recovery work area located in the same building with the DRC. The temporary work area can be used to run business operations when disaster happen.

4.4.2 Backup methods and offsite storage

Backup and recovery method is a means to restore the operating system quickly and effectively when disaster occurs. In this stage, the backup method will be determined, that will be used to increase the availability of corporate data. The result details are shown in Table 7.

JONEC system and data feed system contains applications. Backup method used creates a scheduler to perform replication of applications into backup system in the DRC. The replication process is done every 24 h even if there are no changes in the application.

Remote trading system and back office system contain application and database. Backup method used creates a scheduler to replicate applications and databases into the backup system located in the DRC. The replication process is done every 12 h automatically.

File server using a backup method creates a scheduler that will replicate the backup data into system in DRC. Because the data in the file server are too large, the replication process will be done automatically every 24 h after office hours.

4.5 Recovery procedures

At this stage, a procedure that needs to be done in recovery process would be created when disaster occurs. Recovery procedure is based on reference guidelines BCP exchange members and adapted to the company's standard operating procedure (SOP). The process recovery

Table 6: System recovery priority

Priority	Systems and applications	MTD (min)	RTO (min)	RPO (min)
1	Remote trading system	120	30	1,440
2	Data feed system	120	30	720
3	JONEC system	180	60	1,440
4	Back office system	180	60	720
5	File server	300	180	1,440

Table 7: Backup method

System	Backup method	Backup frequency
JONEC system	Manual backup	Every 24 h
Remote trading system	SQL server backup	Every 12 h
Data feed system	Manual backup	Every 24 h
Back office system	SQL server backup	Every 12 h
File server	Manual backup	Every 24 h

procedures will be assisted with work units that have responsibility in the process of business operations such as compliance unit, risk management, and also the management company. The procedures required in performing the recovery is as follows:

1. DRP activation procedure

   The purpose of the activation procedure is to provide guidance for companies in the activation of DRP. The guide contains an examination of any disruptions that occur, as well as the measures that must be taken to activate the DRP.
2. Emergency response procedures

   This procedure is a guide to the personnel in the emergency response team for the implementation of emergency response activities when disaster occurs, which includes rescue and protection of resources and important assets of the company.
3. Crisis recovery procedures

   This procedure is a guide to the personnel in a crisis recovery team for running the system recovery, infrastructure, and human resources that support the company business operations.
4. Operational procedures during crisis

   This procedure is a guide to the personnel in a crisis operations team for carrying out the activities of recovery of critical business processes that are owned by the company.
5. IT maintenance procedures

   This procedure is a guide for the personnel included in the crisis recovery team for the implementation of recovery systems and IT infrastructure that support the business operations of the company. The main objective of the system maintenance and related IT infrastructure is to ensure that DRP is always kept up to date and in accordance with the company's current condition, complete, accurate, and ready to be implemented under conditions of a disaster.

Prior to the activation of disaster recovery process, the activation procedures must be sufficiently relevant, practical, and actionable. Plan testing is required, but the first step is to check that all activation requirements have been met. To that purpose, activation processes should be developed in accordance with three key guidelines:

1. The scope of activation must include five activation scope keys to guarantee that linked processes are fully actionable (considering DRP scope and specifics).
2. Activation guidelines must concentrate on triggering events and situations in order to properly examine and evaluate present conditions and decide if the DRP should be triggered.
3. Activation steps must be established in order for them to be carried out in a consistent and ordered manner. Everyone should understand what they need to accomplish and how to do it.

Below are five activation scope keys.

The sum of all relevant strategies and processes to guarantee that the DRP may be implemented when required and in an orderly and effective manner, comprising the five parts are listed below:

1. Criteria for activation: identifying the exact crisis circumstances that cause plan activation (according to type, severity, impact, and duration).
2. Evaluation procedures: to assess probable catastrophic occurrences and verify that activation conditions are satisfied.
3. Mechanisms of approval: to get suitable plan activation permissions, taking into account IT management professionals, line of business management personnel, and corporate leaders.
4. Logistics of activation: to guarantee that all facilities and systems, including the specified command center site, are available as required to support the plan activation, including the majority of, if not all, disaster recovery "command and control" tasks.
5. Communication protocols: all activation-related decisions and actions must be communicated to all workers and other interested parties (customers, vendors, suppliers, and the general public).

4.6 Testing and review

Simulated testing needs to be done to test whether the development of DRPs can work well. Simulation testing will be conducted on a Saturday in accordance with the schedule set by the Indonesia Stock Exchange. In the scenario of testing being conducted, in the main office, system does not need to be turned off because the remote trading system cannot work if the system is not connected with the company Indonesia stock exchange system. Team members only need to connect the connection with systems belonging to the Indonesia Stock Exchange in DRC and recovery of data into the system for use and testing. All employees of the company shall participate in the simulation process.

4.7 Documentation

Results of the analysis processes in the development of DRPs that have been made will be documented for the

company. The documentation includes background, DRP organizational structure, risk analysis, BIA, recovery strategies, recovery procedures, and the required supporting documents.

5 DRP implementation

DRP implementations can be done after doing some process that is:

1. Perform simulation testing that accompanied by an independent reviewer.
2. Independent reviewers will conduct an evaluation of DRP testing simulations and prepare a review report.
3. Independent reviewers will present the review report of the DRP testing result to the Indonesian stock exchange.
4. Based on the results of the evaluation carried out, regulator will respond whether the implementation of DRP is approved or not.

After the company received the approval for the implementation of the DRP, the company needs to add DRP design into the company policy. With the design of the DRP, the company can carry out such procedures when a disaster occurs and can minimize the risk accepted.

6 Conclusion and recommendation

Based on the test results for the development and implementation of the DRP in stock exchange industry in Indonesia, it can be concluded that the development of DRP is made and can be implemented and used as a guide in the SOP in the event of a disaster so that employees know what procedures need to be carried out when disaster strikes. This is evidenced by the approval given by the regulator on simulation results of DRP testing. In addition to the DRP, company expects to minimize the impact of disaster and the company also has plans to prepare for and recover human resources and systems information so that company business operations can continue to run the in the event of a disaster.

Recommendations given to the company is to always update the DRP and always adjust to the changes that occur. Company also needs to do simulation testing and review of the DRP to be held at least once a year to check the effectiveness of the DRP.

Acknowledgments: We would like to acknowledge the support and facilities given by Binus Graduate Program as well as Advanced Institute of Industry Technology, Tokyo, Japan during the research.

Funding information: Not applicable.

Author contributions: F.L.G. and A.A. have initiated the study, conducted the experiments, and made the first draft of this article. T.M. gave experts' opinions and contributed to the experimental phase. All authors have read and approved the final manuscript.

Conflict of interest: The authors declare that they have no competing interest.

Ethics approval and consent to participate: Not applicable.

Consent for publication: Not applicable.

Data availability statement: The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

References

[1] Al-Abed GK, Nasereddin HHO. Business continuity based on backup. Am Acad Sch Res J Spec. 2013;5(3):253.
[2] Barnes JC. A guide to business continuity planning. New Jersey, USA: Wiley; 2001.
[3] British Standard. Business continuity management – Part 1: code of practice. London, UK: British Standard Institution; 2006.
[4] Bursa Efek Indonesia. Pedoman business continuity plan Anggota Bursa. Indonesia: Indonesia Stock Exchange; 2012.
[5] Business Continuity Planning And Disaster Recovery Planning. Retrieved June 25, 2020. From http://www.icaiknowledgegateway.org/littledms/folder1/chapter-6-business-continuity-planning-and-disaster-recovery-planning.pdf.
[6] Clitherow D, Brookbanks M, Clayton N, Spear G. Combining high availability and disaster recovery solutions for critical IT environments. IBM Syst J. 2008;47(4):563–75.
[7] Enshasy M. Evaluating business continuity and disaster recovery planning in information technology departments in Palestinian listed companies. Gaza, Palestinian: Islamic Universit of Gaza; 2009.
[8] Hinca M. Business continuity and disaster recovery for IS. Brno, Czech Republic: Masarykova Univerzita; 2006.
[9] Wunnava S, Ellis S. Disaster recovery planning: A PMT-based conceptual model. SAIS 2008 Proceedings; 6. Richmond, VA, USA: SAIS; 2008.
[10] Kadlec C, Shropshire J. Best practices in IT disaster recovery planning among US banks. J Internet Bank Commer. 2010;15(1):1.
[11] Martin BC. Disaster recovery plan strategies and processes. Maryland, USA: SANS Institute InfoSec Reading Room; 2002.

[12] Maulany R. Konsep dan strategi pemulihan bencana terhadap data center menggunakan metodelogi disaster recovery plan (DRP). J Biologic. 2007;6(1).
[13] Michael B. Determining the critical success factors of an effective business continuity/Disaster recovery program in a post 9/11 world: a multi-method approach. M.B.A Thesis, Montreal, Canada, Concordia University; 2006.
[14] Nikolić B, Ružić-Dimitrijević L. Risk assessment of information technology systems. Issues Informing Sci Inf Technol. 2009;6.
[15] NIST Special Publication 800-30. Risk Management for Information Technology System; 2002.
[16] NIST Special Publication 800-34 Rev. 1. Contingency Planning Guide for Federal Information Systems; 2012.
[17] NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments; 2012.
[18] Omar A, Alijani D, Mason R. Information Technology Disaster Recovery Plan: Case Study. Acad Strategic Manag J. 2011;10(2):127.
[19] Putri SW. Pembangunan disaster recovery plan untuk sistem informasi Manajemen Terintegrasi ITB. Bandung, Indonesia: ITB Press; 2008.
[20] Susan S. Business continuity and disaster recovery for IT professionals. Amsterdam, Netherland: Elsevier Inc. All.; 2007.
[21] Utomo BP. Disaster Recovery Plan Implementation In PT. United Tractors Pandu Engineering. Jakarta, Indonesia: Binus University; 2012.
[22] Wijaya L, Dewandi PI. Perancangan dan simulasi hasil disaster recovery Center Pada PT XYZ. Jakarta, Indonesia: Binus University; 2010.
[23] Hanung NP, Nana S, Anugrah PR, Wawa W. Information technology disaster recovery plan (IT-DRP) model-based on NIST framework in Indonesia. Int J Appl Inf Technol (IJAIT). 2019;3(1):34–45.
[24] Hinon G, Manik G. A Review on disaster management and its mitigation techniques. Int J Eng Res & Technol (IJERT). 2020;6(10).
[25] Soni VD. Disaster recovery planning: Untapped success factor in an organization. SSRN. 2020;12(7).
[26] Yu M, Katsuya Y. Survey on post-disaster timelines following a large-scale disaster expected to occur in the near future for pre-disaster recovery planning. J Integr Disaster Risk Manag. 2021;6(3).