IT Disaster Recovery Plan

When a disaster strikes, businesses suffer and are at risk, therefore, one of the goals of business planning is to minimise disruption of product and service delivery to the greatest extent possible. The overarching concern is business continuity.

An IT disaster recovery plan serves as the foundation of a business continuity strategy, and the goal of business continuity is to maintain a minimum level of service while restoring the organisation to normal operations. When disaster strikes, a company that does not have a comprehensive and updated disaster recovery plan risks losing customers to competitors, losing funding, and having the need for its products or services re-evaluated and considered potentially unnecessary.

You are welcome to modify this document to meet your company's DR requirements.

Alternatively, Schedule a FREE DR Discovery call with Consult Circle.

0203 916 5593 | Consult Circle

DR Plan History

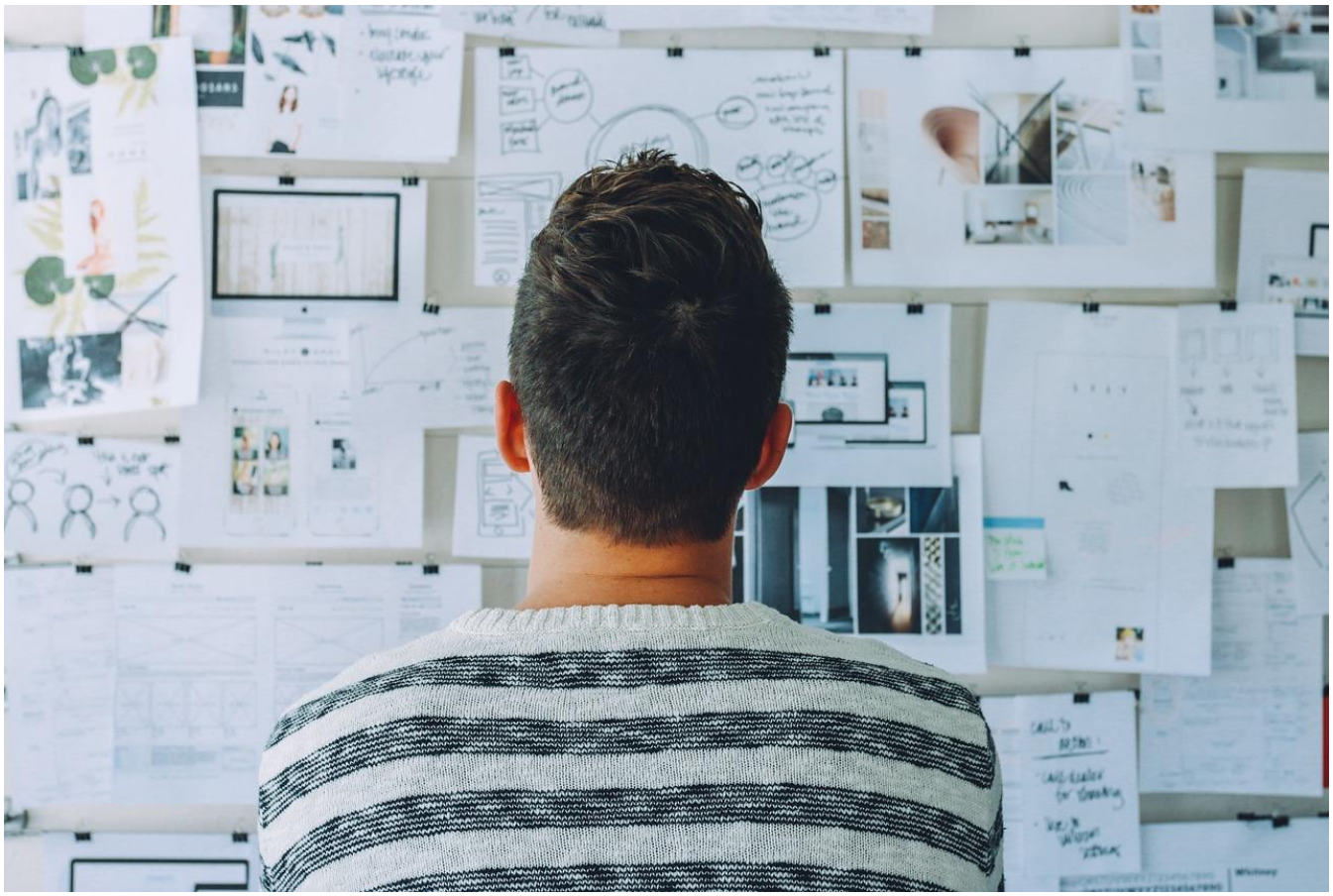
Date	Full name	Description

Table of Contents

Document Outline

This document outlines our technology disaster recovery (DR) policies and procedures, as well as our plans for restoring essential technology platforms and telecommunications infrastructure. This document contains a summary of our recommended procedures. In the event of a real emergency, changes to this document may be necessary to ensure the physical safety of our people, infrastructures, and data.

Our mission is to guarantee the accessibility of information systems, data integrity and availability, and business continuity.



Typical Company DR Policy

- The organisation must create a comprehensive IT disaster recovery plan to determine the requirements
- a formal risk assessment must be conducted for the strategy for disaster recovery
- The disaster recovery plan should consist of all necessary and critical steps in accordance with key infrastructure elements, systems, and network business activities.
- The disaster recovery plan must be kept up to date in order to be effective
- The disaster recovery plan should be tested on a regular basis in a simulated environment in order to ensure that it can be used in real emergency situations
- Both staff and management acknowledge how this will be carried out as well as their own respective roles

Our Objectives

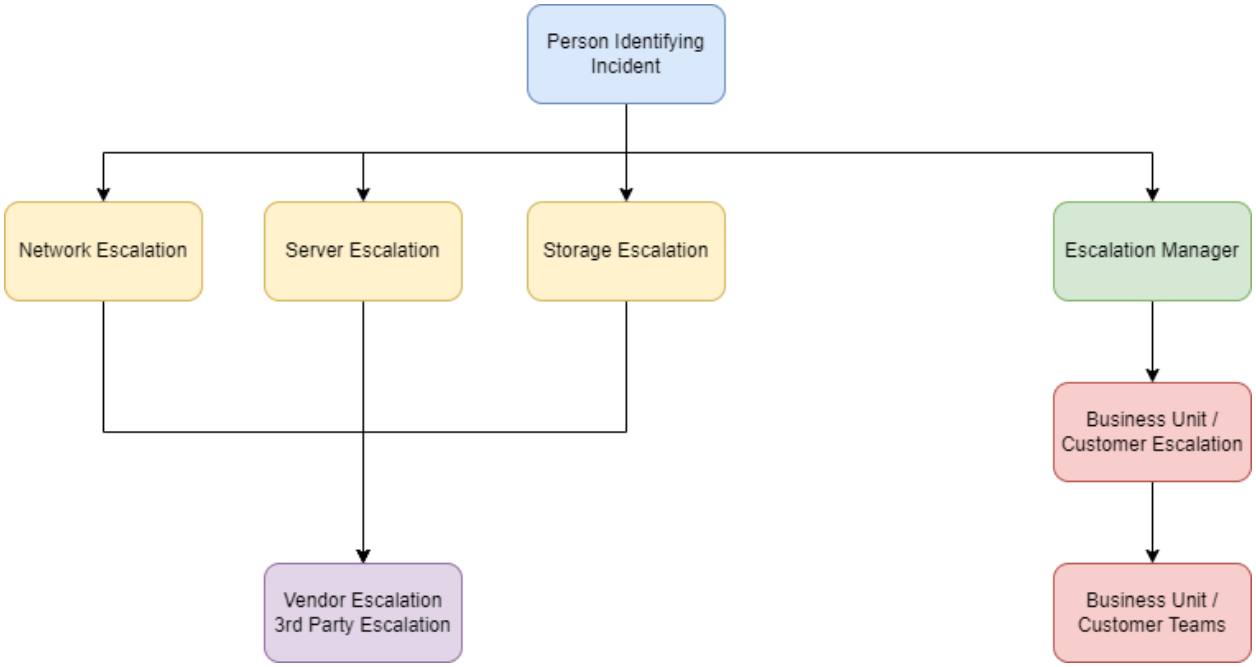
The disaster recovery plan's primary focus is to create, evaluate, and document a structured and comprehensible strategy that will aid the company in recovering as quickly and efficiently as possible from such an unpredicted disaster or emergency that disrupts business operations and information systems. Additional goals include the following:

- The requirement to make sure that all staff fully comprehend their own responsibilities in putting a strategy into action
- The requirement to guarantee that operational policies are observed in all scheduled events
- The requirement to guarantee that contingency plans are cost-effective
- The requirement to take into account the ramifications for all other corporate networks and sites
- Disaster recovery functionality for existing clients, vendors, and others

Key Personnel Contacts

Full Name	Job Title	Phone Number	Email Address

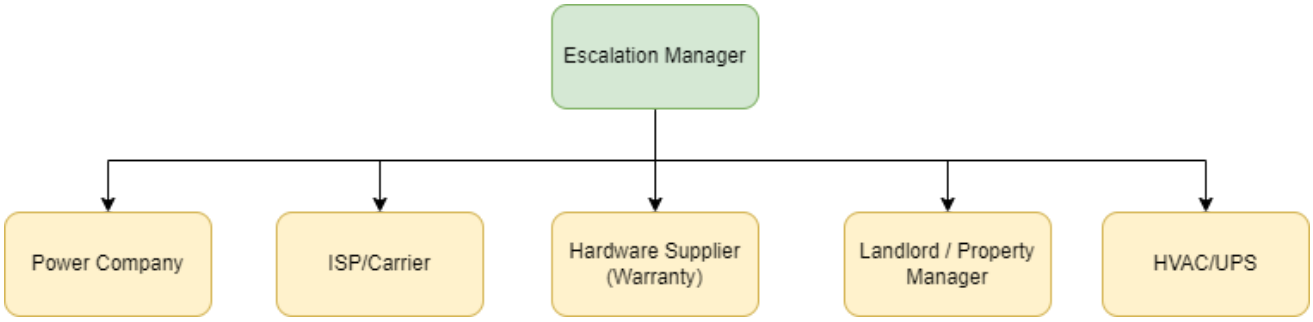
Notification Flow



External Emergency Contacts

Name	Account Number	Contact Options	Contact
Landlord		Work	
		Mobile	
		Email Address	
Power Company		Work	
		Mobile	
		Email Address	
Telecommunications Carrier		Work	
		Mobile	
		Email Address	
Server Supplier		Work	
		Mobile	
		Email Address	
Insurance		Work	
		Mobile	
		Email Address	
HVAC/UPS		Work	
		Mobile	
		Email Address	

External Contacts Flow



DRP Overview

Plan Changes

The DRP updating procedure must be properly implemented and monitored. When adjustments are made to the plan, they must be tested extensively, and necessary adjustments towards the training content must be made. This will entail the use of formalised change control procedures overseen by the IT Director.

Plan Documentation

Backups of the plan, along with Disks and physical copies, will also be kept in safe locations determined by the company. Every member of senior management would be given a Disk and physical copy of the plan to keep at residence. This plan will be distributed to each participant of the Disaster Recovery and the Business Recovery Team on disk and in physical copy.

The master protected copy will also be saved on a specially designated resource base.

Photo by fauxels

Backup strategy

This strategy involves the maintenance of a duplicate site, allowing for immediate swapping between both the live website and the backup site.

The following are the essential business procedures as well as the agreed-upon contingency plan for each.

Key Business Operations	Contingency plan
Tech Support	
Email	
Human Resources	
Finance	
Website	Duplicate website
Call centre	

Risk Management

There are various possible obstructive dangers that can take place at any time and interrupt regular business operations. We've taken into account a broad range of possible threats, and the outcomes of our discussions are discussed in this segment. Each possible environmental disaster or emergency situation has been thoroughly investigated.

The emphasis here is on the degree of disruption in which each type of emergency could cause.

The following possible disasters have been identified:

Potential Disaster	Probability	Impact	Summary of Potential Consequences and Corrective Actions
Flood	3	4	All critical equipment is located on 1st Floor
Fire	3	4	Suppression system installed in main hardware centres. Fire and smoke detectors on every floor.
Tornado	3	4	
Electrical Storm	3	4	
Act of Terrorism	3	4	
Act of Sabotage	3	4	
Power Outage	3	4	Failover UPS array with automatic standby generator that will be tested each week and monitored remotely 24 hours a day, seven days per week. UPS arrays can also be actively monitored.
Server Failure	3	2	
Software Failure	3	3	
Loss of communication services	4	4	
Loss of network services	4	4	
Cyber Attack	4	4	

Probability 1=Very High 5=Very Low *Impact* 1=complete destruction 5=Minimal Damage

Emergency

Activating Emergency Plans

This policy has been created to ensure that during the event of an emergency or disaster, employees know who needs to be contacted. Procedures have been created to make sure that communication can be done quickly while disaster recovery is activated.

The DR plan will primarily rely on members of management and staff who will contribute the managerial and technical expertise required for a seamless technology and business recovery. Distributors of essential services and products will continue to help in the restoration of operational processes as the business resumes normal service.

Events that should alert and trigger the DRP

- Flooding of premises
- Fires
- Power Loss
- Earthquakes
- Hardware Failure
- Loss of internet connectivity
- Denial of Service Attacks

Assembly Points

Emergency routes and exits must lead as directly as possible to a place of safety Immediately proceed to the Assembly Point in the event of the premises being exposed to serious, imminent and unavoidable danger
In the need of total evacuation of the premises there needs to be an appointed Primary Assembly Point and Secondary Assembly Point.

- Primary Assembly Point: Car park (good distance away from the premises)
- Secondary Assembly Point: ……..

Escalation Process

In the case of an emergency the Emergency Response Team's role is to decide which Disaster Recovery Plan needs to be activated to best respond to the emergency
Their responsibilities include:

- Immediately respond to a potential threat or disaster by contacting Emergency services
- Determine the magnitude of the emergency and its impact on the business, data centre, and other key infrastructure
- Determine which Disaster Recovery Plan components should be initiated
- Form and manage a disaster recovery team to maintain essential functions and the resumption of normal operations
- Notify the workforce and assign duties and actions as needed.

Disaster Recovery Team

The ERT will contact and assemble the Disaster Recovery Team. The following are the team's responsibilities:

- Providing emergency service facilities within 2 business hours
- Recover critical services within four hours of the emergency
- Return to normal operations within 8 to 24 hours of the incident.
- Work collaboratively with the disaster recovery team, emergency workers, and other stakeholders
- Inform and update the emergency response team

Alert

When an emergency is found, the responsibility falls to the person who has found the incident to contact and alert the Emergency Response team (ERT). They should have access to the contact details to the emergency response teams and who to call if they do not respond. The Emergency Response Team will be responsible for initiating the correct Disaster Recovery Plan for the incident.

ERT	Contact Number

Notifying the Disaster Recovery Team of an urgent situation is one of the initial tasks during the early phases in an emergency situation. The alert will request Disaster Recovery Team members to gather at the location of the emergency and will include enough information to effectively communicate this request. Senior representatives from the major business departments will form the Business Recovery Team.
The Business Recovery Leader should be a senior figure of the company's leadership team, in charge of overseeing the procedure and ensuring that normal business operations resume as promptly as possible.

DRP Management Procedures

Members of the management team will keep a hard copy of the names and contact numbers of each employee in their departments. In addition, management team members will have a hard copy of the company’s disaster recovery and business continuity plans on file in their homes in the event that the headquarters building is inaccessible, unusable, or destroyed.

Contacting Employees

Assigned staff members will contact other personnel to explain the emergencies as well as the business's current plans. Staff members who have been unable to reach personnel on their contact list are advised to consult the staff member's emergency number to convey disaster information.

Contingency Staff

If a manager or employee who have been assigned to contact other members of staff is absent or incapacitated, the assigned standby employee will undertake update duties.

Updates

Employees can call a contact number listed on the DRP contact list for specific updates on the incident. Updates will contain details about the extent of the emergency, assembly locations, and alerts on work resumption.

Contacting emergency contacts and family members

If the emergency leads to a situation (if someone is hospitalised or injured) in which an employee's family or emergency contact need to be contacted, it is vital to do so quickly.

Media

Speaking with Media

Staff will collaborate with the media in accordance with previously authorised and declared guidelines to deal with communicating after an incident has been controlled

Media procedures

- Avoiding negative publicity
- Seize opportunities for beneficial publicity
- Know the answers to the following fundamental questions:
  • What occurred?
  • What caused it?
  • What are your plans to address it?

Regulations for Interacting with Media

Only the media department is authorised to communicate with the press directly; anyone else approached must refer incoming calls or in-person members of the media to the media department.

Insurance

The company's disaster recovery and business continuity strategy include insurance policies. These policies cover the following

- errors and omissions insurance
- directors and officers' liability insurance
- general liability insurance
- business interruption insurance

If insurance-related support is required after an incident outside of regular office hours, make sure to contact: ……..

Policy Name	Cover Type	Cover Period	Amount of Cover	Person responsible for cover	Renewal date

Financial Assessment

The emergency response team must prepare an initial evaluation of the incident's repercussions on the company's finances.
The evaluation should include:

- Loss of financial records
- Revenue loss
- Loss of cash, credit cards, etc.

Financial Needs and Requirements

The company's immediate financial requirements must be addressed. These are examples:

- Cash flow position
- Temporary borrowing capability
- Impending payments for taxes, Social Security, etc

Legal Assessment

The company's legal team and Emergency Response Team will collaboratively review the incident's repercussions and determine whether there may be legal actions arising from the incident; particularly, the likelihood of claims against the company for regulatory violations, etc.

Disaster Recovery Plan Training

Disaster recovery plan training is an important component of the planning process. Everyone who partakes in a Disaster recovery plan exercises learn - what should be improved and how the adjustments can be incorporated. DRP exercises make sure that emergency teams are well-acquainted with their responsibilities and, more importantly, confident in their abilities and role in the case of an emergency.

When disaster strikes, successful disaster recovery plans go into effect seamlessly and effectively. This will only occur if everyone involved in the strategy has trained and learnt their roles. The plan should be ascertained by mimicking the conditions under which it must operate and observing what happens.

Disaster Recovery Plan Templates

Technology Disaster Recovery Plan

System Template 1

RTO	4 hours
RPO	2 hours
Contracted frequency of DR tests	Annual

System Name	
Overview	
System	Location: Model: Operating System: CPUs: Memory: Total Disk: Name: Serial: DNS Entry: IP Address:
Primary Site	
Secondary Site	
Applications	
Associated Servers	

Key Contacts	
Hardware Vendor	
System Owners	
Database Owner	
Application Owners	
Software Vendors	

Backup Template 1

RTO	4 hours
RPO	2 hours
Contracted frequency of Backup tests	Annual

BACKUP STRATEGY FOR SYSTEM ONE	
Daily	
Monthly	
Quarterly	
SYSTEM ONE DISASTER RECOVERY PROCEDURE	
Scenario 1 Total Loss of Data	
Scenario 2 Total Loss of HW	

File Systems

File System	File system Mounted on	MB/GB Used	Available	%Used
Minimal file systems to be created and restored from backup:				
Other critical files to modify				
Necessary directories to create				
Critical files to restore				

Technology Disaster Recovery Plan (Second System)

System Template 2

RTO	4 hours
RPO	2 hours
Contracted frequency of DR tests	Annual

System Name	
Overview	
System	Location: Model: Operating System: CPUs: Memory: Total Disk: Name: Serial: DNS Entry: IP Address:
Primary Site	
Applications	
Associated Servers	

Key Contacts	
Hardware Vendor	
System Owners	
Database Owner	
Application Owners	
Software Vendors	

Backup Template 2

RTO	4 hours
RPO	2 hours
Contracted frequency of DR tests	Annual

BACKUP STRATEGY FOR SYSTEM TWO	
Daily	
Monthly	
Quarterly	
SYSTEM TWO DISASTER RECOVERY PROCEDURE	
Scenario 1 Total Loss of Data	
Scenario 2 Total Loss of HW	

File systems

File System	File system Mounted on	MB/GB Used	Available	%Used
Minimal file systems to be created and restored from backup:				
Other critical files to modify				
Necessary directories to create				
Critical files to restore				

Local Area Network (LAN) Disaster Recovery Plan

LAN Template 1

RTO	4 hours
Contracted frequency of DR tests	Annual

System Name	
Overview	
Switches and Routers	Location: Model: Version: Name: Serial: DNS Entry: IP Address:
Primary Site	
Applications	
Associated Servers	

Key Contacts	
Hardware Vendor	
System Owners	
Database Owner	
Application Owners	
Software Vendors	

Wide Area Network (WAN) Disaster Recovery Plan

WAN Template 1

RTO	4 hours
Contracted frequency of DR tests	Annual

System Name	
Overview	
Switches and Routers	Location: Model: Version: Name: Serial: DNS Entry: IP Address:
Primary Site	
Applications	
Associated Servers	

Key Contacts	
Hardware Vendor	
System Owners	
Database Owner	
Application Owners	
Software Vendors	

Remote Connectivity Disaster Recovery Plan

Remote Template 1

RTO	4 hours
Contracted frequency of DR tests	Annual

System Name	
Overview	
Server, Switches and Routers	Location: Model: Version: Name: Serial: DNS Entry: IP Address:
Primary Site	
Applications	
Associated Servers	

Key Contacts	
Hardware Vendor	
System Owners	
Database Owner	
Application Owners	
Software Vendors	
Offsite Storage	

Communications Disaster Recovery Plan

Comms Template 1

RTO	4 hours
Contracted frequency of DR tests	Annual

System Name	
Overview	
Server, Switches and Routers	Location: Model: Version: Name: Serial: DNS Entry: IP Address:
Primary Site	
Applications	
Associated Servers	

Key Contacts	
Hardware Vendor	
System Owners	
Database Owner	
Application Owners	
Software Vendors	
Offsite Storage	

Disaster Recovery Forms

Damage Assessment Form

Affected Business Processes	Description	Extent of Damage

Form for Managing Disaster Recovery Operations

- All procedures will be determined using a standardised format during the disaster recovery process.
- Where reasonably possible, this plan will need to be revised regularly throughout the disaster recovery phase
- All measures taken during this process must be documented.

Measure Taken:
Reference Number:
Description:

Date/Time Undertaken	Date/Time Completed	Resources Used	Team Leader Name

Disaster Recovery Event Recording Form

All significant activities that take place during the disaster recovery period must always be documented.

- The disaster recovery group leader must keep a log file.
- This activity log should always be started as soon as the incident begins, and a duplicate of the log must be given to the business recovery team once the immediate threats have been eliminated.
- The disaster recovery group leader must fill out the following activity log to document all significant events throughout disaster recovery until responsibility is transferred to the business recovery team.

Incident Description:
Start Date:
Date & Time DR Team Dispatched:

Date/Time DR Team Concluded:
Date/Time BR Team took charge:

Disaster Recovery Response Form

After the initial disaster recovery response is completed, the Disaster Recovery Team leader must produce a report on the actions that were carried out.

- The report should include details about the incident, who had been alerted and when, the measures taken by Disaster Response Team members, and the results of those decisions.
- The report should include a view of the effects on core business operations.
- The report must be handed to the team leader of the business recovery team, with a duplicate sent to senior leadership as needed.
- Following the completion of the required disaster recovery response, the Disaster Recovery Team leader will prepare a disaster recovery report.
- The report will be sent to senior leadership along with the company's business recovery team leader.

This report should include the following:

- Dates and times of everyone who has been alerted of the incident
- Decisions made by Disaster Recovery Team
- The results of actions taken.
- A determination of the repercussions on regular business operations.
- Evaluation of the Business continuity Plan effectiveness
- Lessons Learned

Mobilisation of Disaster Recovery Team

- Following an incident that necessitates the restoration of technology infrastructure assets, the DRT should be alerted and placed on constant alert.
- The template seen below can be utilised to document the mobilisation of the Disaster Recovery Team after the impact assessment and emergency response teams have completed their work.

Incident Description:
Start Date:
Date & Time Disaster Recovery Team Concluded:

Team Member Full Name	Contact Details	Date/Time Contacted	By Whom	Response	Start Time/Date

Additional Relevant Details:

Mobilisation of Business Recovery Team

- Following an incident that necessitates the mobilisation of the disaster recovery team, the business recovery team must be alerted and placed on constant alert.
- Once the disaster recovery team's work is completed, the template seen below will be followed to record the deployment of the business recovery team.

Incident Description:
Start Date:
Date & Time Business Recovery Team Concluded:

Team Member Full Name	Contact Details	Date/Time Contacted	By Whom	Response	Start Time/Date

Additional Relevant Details:

Business Recovery Task Progress Form

- During this time, the advancement of both business and technology recovery tasks should be closely monitored.
- Because problems encountered by each team may have a significant impact on other dependent tasks, it is crucial to ensure that every task is properly resourced and that the efforts needed to restore regular business operations are not underestimated.

Measures Taken	Person(s) Accountable	Estimated Completion Time	Actual Completion Time	Progress Made	Additional Relevant Details
1.					
2.					
3.					

Business Recovery Report

- When business recovery tasks have been undertaken, the Business Recovery Leader must produce a report on the tasks that were conducted and executed.
- The report must include details about the incident, who had been alerted and when, the measures undertaken by the Business Recovery Team, and the results of those tasks.
- The report should also include an evaluation of the influence on regular business operations.
- The document should be sent to senior leadership.

This report should include the following:

- An explanation of the event.
- Times, dates and names of individuals who have been alerted of the incident.
- Actions undertaken by the business recovery team as well as the outcomes of actions taken.
- An evaluation of the impact on business operations.
- Identification of all issues encountered.
- Suggestions for improving the disaster recovery and business continuity plan.
- Lessons learned

Communications Form

- It is critical that all impacted individuals and organisations are kept fully informed during disaster recovery and business recovery.
- All members must be provided with timely and reliable information.
- Any forecast of when normal working operations will resume must be declared with carefulness.
- It is also critical that only authorised individuals handle media inquiries.

Affected Parties	Designated Communications Person Full Name	Designated Communications Person's Position	Contact Details
Customers			
Management & Staff			
Suppliers			
Media			
Other Stakeholders			

Returning Authority to Business Unit Management

- Once regular business operations have been restored, responsibility for particular tasks must be returned to the business unit manager.
- This procedure should be formalised to make sure that all stakeholders are aware of the transition in authority and the return to regular operations.
- During the recovery process it is common that authority is handed to the Business Recovery Team Leader
- It is likely that business unit management will also be directly involved throughout the recovery period; however, in order for the recovery process to be efficient and successful, overall responsibility should most likely be with a Business Recovery Team until the recovery period is over.

Business Process and Recovery Completion Form

For each operation recovered, the business recovery team leader and the responsible business unit leader must fill out and submit the following transition form.

A form for each recovered business process should be completed.

Business Process	
Work Conclusion Date Provided by the Business Recovery Team (BRT)	
Date of Transition Back to Business Unit Management	
I confirm that the work of the business recovery team has been completed in accordance with the disaster recovery plan for the above process, and that normal business operations have been effectively restored. BRT Leader Name: ……. Signature: …… Date: ……/……/…… (Any relevant comments by the BRT leader in connection with the return of this business process should be made here.)	
I confirm that the above business process is now acceptable for normal working conditions. Title: …… Name: …….. Signature: …… Date:……/……/……..	

You are welcome to modify this document to meet your company's DR requirements.

Alternatively, Schedule a FREE DR Discovery call with Consult Circle.