



CIO's Guide to
**DISASTER RECOVERY
PLANNING**

Bonus: *BCDR Tabletop Exercise*

Introduction

The types of disasters and their impacts on an organization and its business continuity are varied. Having a well-crafted IT disaster recovery plan and business continuity plan is essential to ensuring your organization can efficiently and effectively resume business operations and recover critical technology needs after a disaster event.

Outages can result in the loss of data such as emails, accounting data, patient or client files, or company records. Not only can this lead to financial loss, but outages present other threats like reputational loss and increased GRC (governance, risk, and compliance) risks.

In this guide, we highlight the key areas of disaster recovery that your organization needs to address to ensure downtime is minimized and recovery is as efficient as possible.

01 Disaster Recovery Planning Guide

02 Disaster Recovery Plan Checklist

03 BCDR Tabletop Exercise

CIO's Guide to Disaster Recovery Planning

Section 1 – Identify

Locations

Identify the locations for all systems, equipment, employees, and services per department.

Assets

Assets for a disaster recovery plan may overlap with a business continuity plan, but it is critical to document hardware, software, application/workloads, and stakeholders by department. Be sure to include any special hardware or software requirements, such as a licensing dongle for a particular application. One thing many businesses overlook is the grouping of servers or assets to provide a single application.

Network configuration

Recording network hardware and software types and configurations will assist during disaster recovery and in the event of a malware issue, hardware failure, or replacement. Network configurations are essential for proper application communications.

Recovery strategies and sites

By identifying locations for assets, you can accurately define recovery strategies and recovery locations for each site in your organization. Depending upon the type and length of potential disasters and regulatory requirements, your organization's needs will vary.

Section 2 – Define

Risk assessment

Risk assessments should flow top-down and back to the top. Each department owns its asset list and reports based on criteria determined by the business. The first of these is disaster potential related to location and impacts, then determining what constitutes a necessity to activate a DR plan.

Business impact analysis (BIA)

A BIA varies based on the type of business you have, so determine the critical revenue or performance indicators and then distribute those based on the bottom line, shareholders, customers, and employees, as appropriate. Having thousands of hourly employees without work and no plan is not a good outcome and could affect business reputation.

Tiers for applications

Without identification, analysis, and a BIA from each department, you will not be able to identify tiers for applications effectively. Closely aligned with RTO/RPO, defining tiers allows disaster recovery processes to recover systems (by application group, if applicable) in the correct order according to business objectives.

RPO/RTO

Determining the recovery point objectives and recovery time objectives, per application and department, is essential to disaster recovery overall.

Application key players

No one knows if applications are functioning better than their developers, owners, and users. Identify and engage these people as part of your regular DR testing.

Failover plan

When you define locations, tiers, and risks, determine your failover plans. They put everything into action. Then consider a fallback plan—how to get back to your production environment. The failover plan may be the most important “do this, now” part of any disaster recovery plan. Communicate these steps to your DRaaS provider, executives, or anyone who needs to know.

Response operations

During a crisis, having a central location/entity for all recovery operations enables better communication, reduces duplications, makes checklist communications more efficient, and streamlines communications to executives and the public. Dedicate a person or a team to facilitate this role, and use it.

Section 3 – Document

Document everything

Sections 1 and 2 gather and define information. You must document all items during these phases of creating a disaster recovery plan and do so with the mindset that it will be read during a crisis and potentially by anyone. Avoid using slang, acronyms, or familiar jargon.

Contact information

Assume no one has access to the team, department head, or executive contact information. This information is helpful for cross-organization communication, new employees, or third-party assistance. Set up call trees for each department so each person knows who is responsible for contacting whom. Include hardware, software, and application vendors and support numbers, as well as those for any contractors currently working with your organization.

Access Control Lists (ACL)

Generally, systems will maintain ACLs when recovered from a backup or as a replicated workload. During a crisis, administrators and employees may need additional permissions to assist with recovery or reduced permission to remove risk. Additionally, consider physical access needs with relation to buildings, servers, and IT equipment.

Recovery checklists

Create checklists for each department or application for use during disaster recovery. Response operations team members may complete these lists as part of crisis management, but checklists are crucial to ensure you do not miss items.

Store offsite, provide copies to DRaaS provider

Giving a current copy of your DR plan to your DRaaS provider solves two problems at once. You will always have a copy of it offsite in an accessible location, and you will be updating your provider regularly, ensuring the best response possible.

Section 4 – Test

Critical to test

Testing the disaster recovery plan is critical. Testing is the only way to know if your documentation and processes make sense and are complete and if backups and replications are reliable. You should test quarterly, annually, and possibly whenever any significant changes occur.

Peer testing

Allow others to perform tests or at least review the documentation and processes. Doing so will prevent confusion and find anything potentially overlook or skipped because it makes sense to the person writing the documentation but may not to the person executing the plan.

App owners, users, public

Have different groups of users perform acceptance testing, as experiences and expectations vary.

Section 5 – Refine/Revise/Repeat

Refine steps as necessary

Disaster recovery plans should be living documents. Make it a routine procedure to update the plan.

Continue to update regularly

Employee turnover, changes to the environment, or even overall business objective changes will affect your disaster recovery plan.

Repeat the DR plan review

When making significant changes to the plan, be sure to have someone review it again. Accidentally deleting a paragraph could have a substantial impact on the overall process.



Disaster Recovery Plan Checklist

Use the outline below to create a Disaster Recovery Plan for your company.

Section 1 – Identify

- Locations
- Assets – by department
 - Hardware
 - Software
 - Applications/workloads
 - Stakeholders
- Network configurations
- Recovery strategy and sites

Section 2 – Define

- Risk assessment – by department
 - By location/type of disaster, duration
 - What constitutes a disaster/plan activation?
 - Distance between physical locations (if not cloud)
- Business impact analysis (BIA) – financials, customers, employees
- Tiers for applications – 1/2/3, etc.
- Recovery point objective (RPO)/Recovery time objective (RTO) for each application
- Application key players
- Failover plan
- Response operations
 - Crisis management and communications

Section 3 – Document

- Everything
 - Section 1 and 2 items
- Contact information
 - Call tree
 - Vendors
 - Contractors
- Access control lists (ACLs)
- Recovery checklists
- Store offsite, provide current copies to DRaaS provider

Section 4 – Test

- Critical to test
 - Quarterly
 - Annually
- Peer testing (someone unfamiliar with the plan or systems)
- App owners, users, public

Section 5 – Refine/Revise/Repeat

- Refine steps as necessary
- Continue to update regularly
 - Employee turnover
 - MACDs (move/add/change/delete)
- Repeat the DR plan review

Dataprise BCDR Tabletop Exercise

Introduction

This exercise is designed to spark discussion within your IT department on your organizational preparedness for a disaster event in the highlighted scenario and provide tangible guidance on areas to improve.

Getting Started

How To Use This Exercise

Tabletop exercises are designed to help organizations walk through potential disaster event scenarios, evaluate business continuity and disaster recovery posture, and identify potential gaps.

This exercise is meant to be a constructive and convenient tool that can be completed within 30 minutes. We recommend the tips below to provide the most value to your organization:

1. Involve all relevant IT stakeholders
2. Tailor the scenario to best match your environment
3. Determine a single facilitator for the exercise
4. Encourage discussion about how your organization would handle the scenario
5. Document your responses to the key questions
6. Develop a plan to close any gaps identified during the exercise

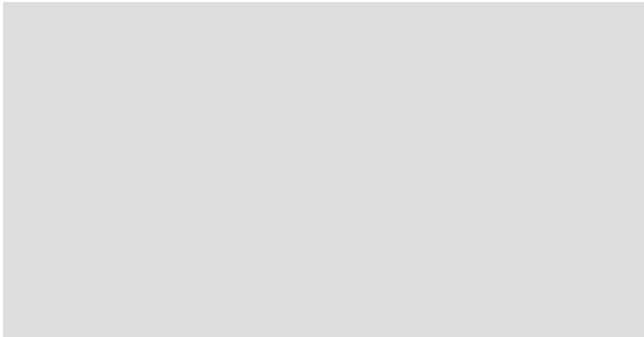


Scenario Set-Up:

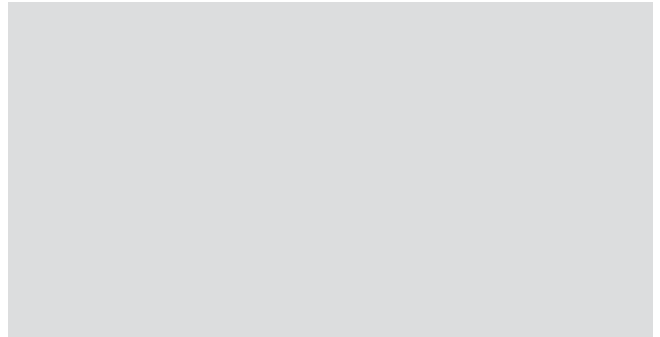
A third-party vendor is facing critical technical issues. This has led to deletion of your organization's critical data and has removed your access to your company's server.

Questions to Discuss

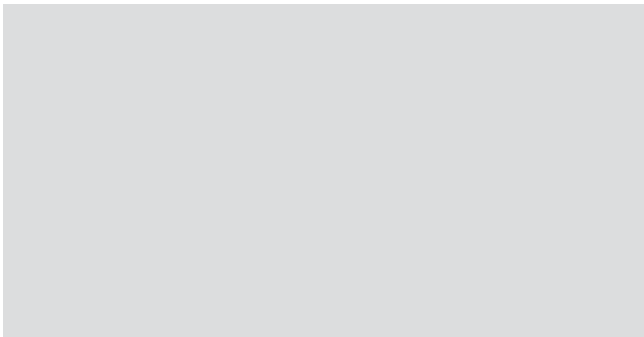
1. What do you do first?



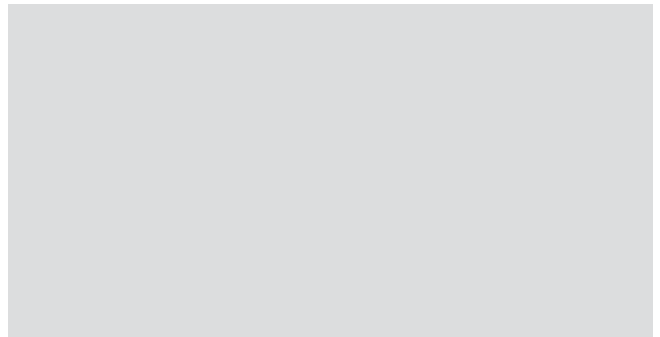
2. How do you determine the impact and criticality of the damage?



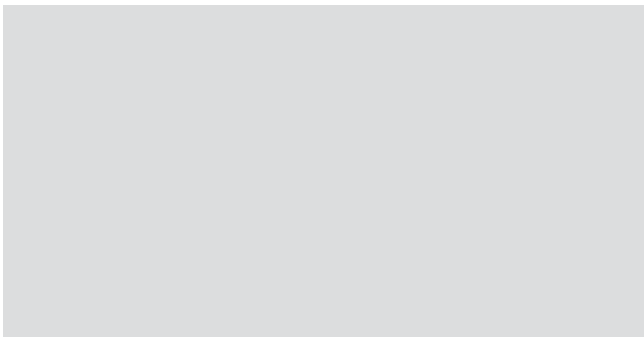
3. How much downtime can you experience before significant harm to the business occurs?



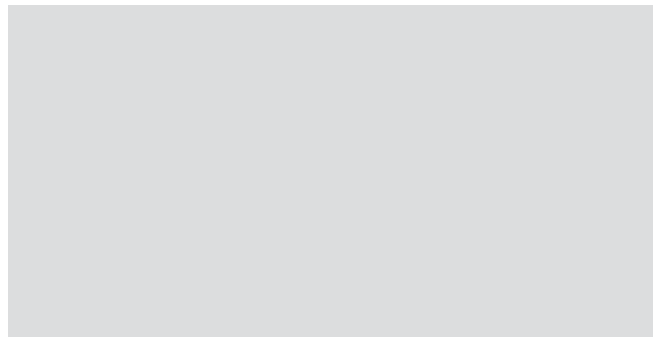
4. What is your recovery process and who is responsible for executing?



5. Who do you notify about the event?



6. What steps will you take to reduce risk and downtime in the future?



Review

How did you do?

Below are some critical components that business continuity and disaster recovery experts recommend should be included as part of your BCDR program.



1. What do you do first?

Recommendations:

The first step your organization should take is to review your Business Continuity plans (BCP) and IT Disaster Recovery plans (DRP), which should be accurate and up to date. If you do not have a BCP and DRP, or they are out of date, ideal first steps include conducting a Business Impact Analysis (BIA) to:

- **Identify the direct cost and revenue impacts**
 - Loss of revenue
 - Loss of productivity
 - Increased operating costs
 - Financial penalties
- **Identify the intangible goodwill, compliance, and safety impacts**
 - Impact on customers
 - Impact on staff
 - Impact on business partners
 - Impact on health and safety
 - Impact on compliance
- Estimate the total impact of downtime
- Develop business down time tolerance
- Develop recovery time objectives (RTO) and recovery point objectives (RPO) tiers
 - RTO refers to how much time an application can be down without causing significant damage to the business
 - RPOs refer to your company's data loss tolerance: the amount of data that can be lost before significant harm to the business occurs
- Identify appropriate (right-sized) recovery time objectives for each service

The goal is to collectively identify which areas of your organization are of greatest importance to the business and key stakeholders' intended strategic direction, thereby enabling your organization to appropriately identify spend levels and prioritize application recovery order.

2. How do you determine the impact and criticality of the damage?

Recommendations:

Ideally you have fully documented your hardware and software assets, including licensing information, and system configurations. Applications and systems that are critical to business success and any dependencies should be categorized by level of criticality (e.g., Tier 1, 2, 3). Your business can leverage this scoring criteria to establish the estimated impact of downtime for each application.

3. How much downtime can you experience before significant harm to the business occurs?

Recommendations:

Define the desired RTOs/RPOs based on the impact and the tolerance for downtime and data loss. Some applications can be down for days without significant consequences, while others can only be down for a few seconds without incurring employee irritation, customer anger, and lost business.

This shouldn't be based on gut feelings — the end goal is to inform your disasterrecovery process and to also have a financial impact roughly estimated for each type of outage.



4. What is your recovery process and who is responsible for executing?

Recommendations:

Your DR deployment model, DR technology requirements to meet RTOs/RPOs, and plans for extended outages (e.g., longer than one month) should be defined in your DRP. Recovery procedures should be documented for each application and system, including identifying required dependencies. The members of your DR team are identified and clearly understand their roles and responsibilities, as well as have access to required passwords and account privileges to execute recovery procedures.

Procedures to operate out of the DR environment (e.g., for executing backups and system maintenance after the failover has been completed), repatriation procedures (e.g., failing back to the primary site), and vendor roles and responsibilities are all documented.

5. Who do you notify about the event?

Recommendations:

Internally, you should identify the stakeholders that are impacted by the incident, your recovery team, or anyone else who may need to become involved, such as the legal team. Depending upon your industry, you may have requirements to report the event to governing bodies and federal agencies. Review the compliance standards you are held to and have a communication plan in place. External communications with customers and suppliers are merited when they are directly affected by any downtime.

This should be a fully fleshed-out communication matrix, and staff should have easy access to this in the case of an emergency.

6. What steps will you take to reduce risk in the future?

Recommendations:

To recover from a disaster event effectively and efficiently, you need a comprehensive DRP and BCP in place that is concise and easy-to-use, incorporating flowcharts, checklists, and diagrams rather than dense manuals. It is important to note the distinction between Business Continuity and Disaster Recovery. Business Continuity planning is about ensuring your business operations can continue at a higher level in the event of a realized risk. A Disaster Recovery Plan outlines specific steps to take to recover the technology needs of your organization after a disaster.

Following an outage, there is a formal post-incident debrief process that includes documenting lessons learned and assigning corrective action items. Ideally your organization's plans should be revisited on an annual basis to keep it up to date regarding levels of criticality, processes, personnel, and stakeholders.

Based on your answers above, determine if there are gaps in your current program and use that information to create an action plan to remediate. If you are uncertain of the adequacy of your organization's DRP, Dataprise's Disaster Recovery Maturity Assessment assesses more than 50 metrics to identify areas that need improvement, and we can provide a roadmap of activities to elevate the maturity of your IT Disaster Recovery Plan.



LET'S TALK!

1.888.519.8111

www.dataprise.com



Why Dataprise?

Founded in 1995, Dataprise is the leading strategic IT solution provider to IT leaders who believe technology should allow you to be the best at what you do.

Our broad solution portfolio is tailored to the needs of strategic CIOs and provides best-in-class managed cybersecurity, data protection, managed infrastructure, cloud, and managed end-user services that transform business, enhance user experiences, and eliminate risks.

We Enable Strategic IT Leaders to Focus on Their Mission

At Dataprise, we handle the technology, so you can focus on your organizations mission. We leverage our in depth knowledge of your industry talent, and our best-in-class service to provide you with a winning formula to help your business succeed above its competitors.

We Have a Deep Pool of Expertise

With over 300+ certified IT experts skilled in technologies across cybersecurity, cloud, infrastructure, mobility, and more, our team works with your organization to ensure your IT challenges are tackled efficiently and effectively.

We Deliver Integrated, Resilient Solutions

We manage and support effect, resilient IT infrastructure that enables CIOs to focus on their strategic priorities to compete with unique advantages in their markets. Dataprise does this by leading with cybersecurity, the only way to protect a company and its sensitive data. While our services are comprehensive and integrated, they are also modular, so companies with some internal IT resources can get the help they need in specific areas.