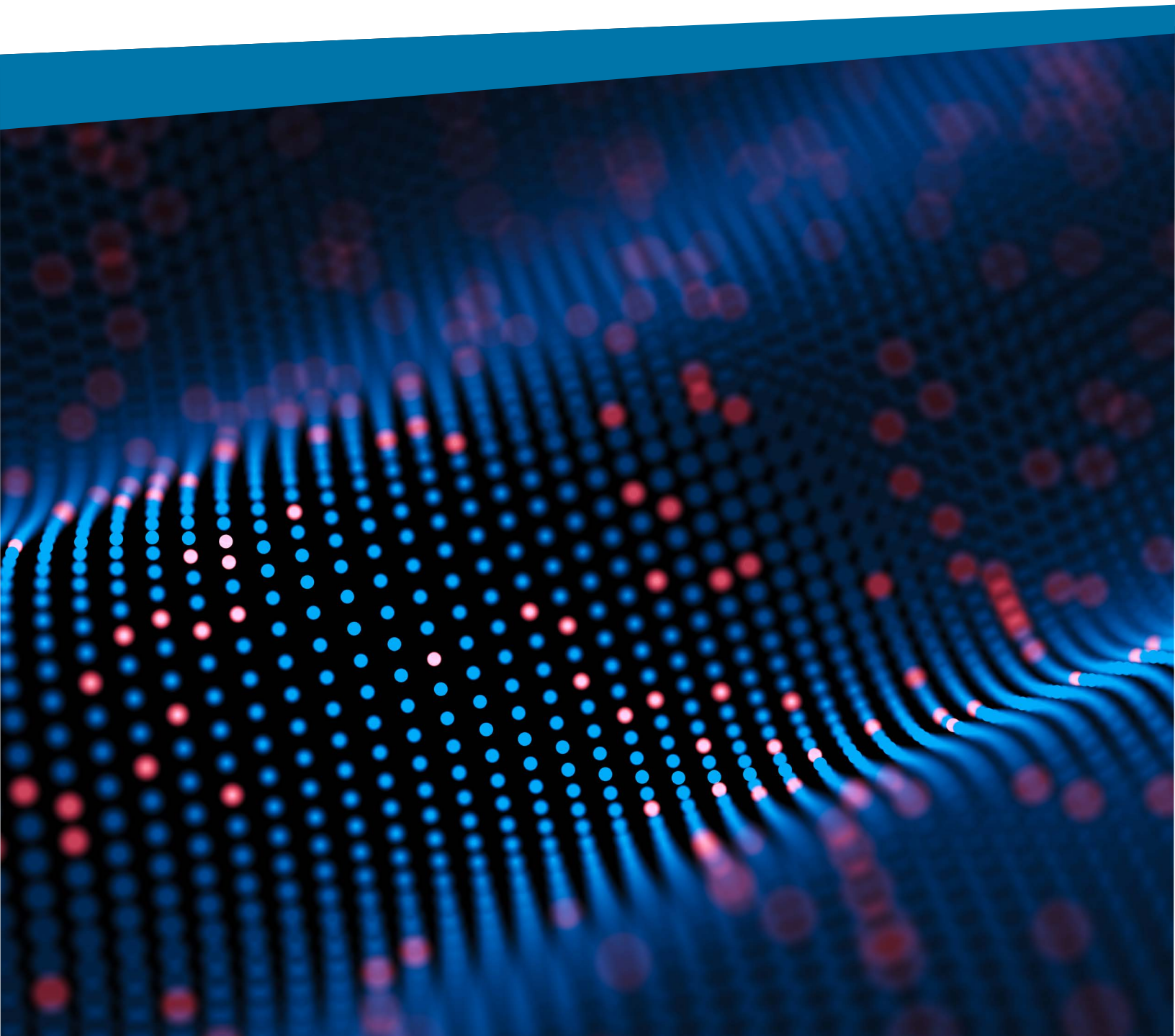
DATAPRISE

Dataprise BCDR Tabletop Exercise Guide:

Critical Data Loss



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.

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

Copyright 2021 © Dataprise.

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?

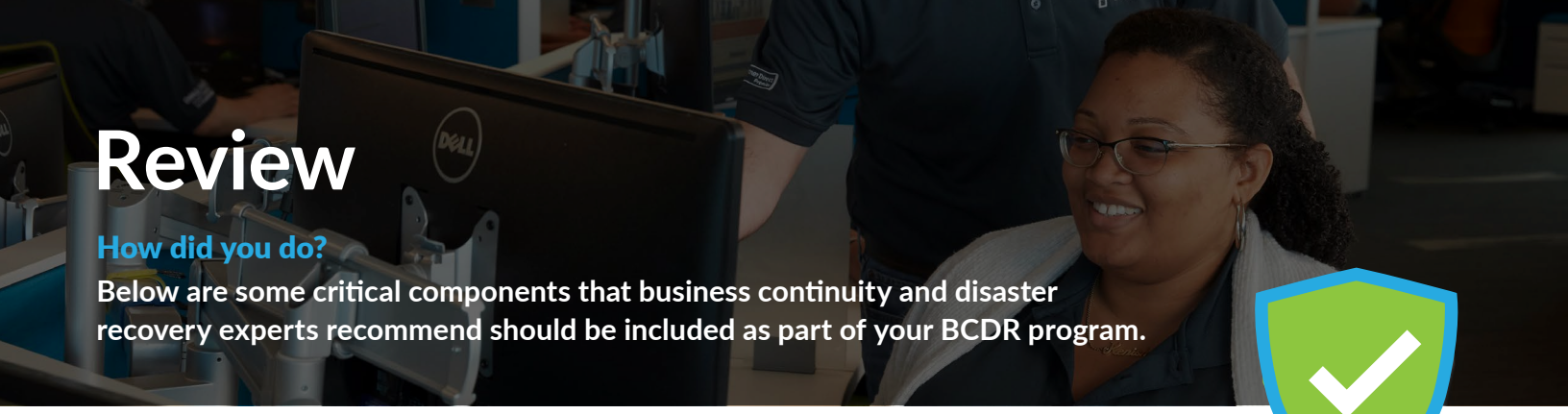
3. How much downtime can you experience before significant harm to the business occurs?

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?

Copyright 2021 © Dataprise.



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 signifi cant 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.

Copyright 2021 © Dataprise.

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 nd 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.

Copyright 2021 © Dataprise.

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 BCDR!

Visit Us:

www.dataprise.com

Call Us at 1.888.519.8111

About Dataprise

Founded in 1995, Dataprise is the leading strategic IT solution provider to midmarket IT leaders who believe technology should allow you to be the best at what you do. Dataprise's unbeatable IT solutions and services are tailored to the needs of strategic CIOs and provide best-in-class managed security, network, infrastructure, collaboration, mobility, and end-user solutions. Dataprise has offices across the United States to support our clients.

Copyright 2021 © Dataprise.