Axcient

Disaster Recovery Plan Template and Guide for MSPs

Introduction

Successful business continuity and disaster recovery (BCDR) depends on a documented disaster recovery plan that is current and comprehensive. With the continuing rise of data breaches primarily targeting servers, recovering data through a disaster recovery plan is more important than ever. A disaster recovery plan template gives MSPs and SMBs a starting point for constructing a detailed plan for responding to a cyberattack, natural disaster, system failure, or other catastrophic data loss incident.

Thorough planning is vital for running a modern business, as many events can affect business continuity. A comprehensive recovery plan is the most effective way to respond promptly to a data disruption and avoid intolerable consequences for your clients. To help, Axcient has created two disaster recovery plan templates – a DR Plan Technical Template and a DR Plan SLA Template. These templates are customizable to fit your MSP, providing each client with a rinse-and-repeat DR plan process. Download the templates below and keep reading to learn more about disaster recovery planning.

> Download the DR Plan Technical Template
>
> Download the DR Plan SLA Template

What is a Disaster Recovery Plan?

A disaster recovery plan (DRP) outlines a company's repose to significant disruptions caused by malicious actions, natural events, or human mistakes. This plan is a detailed guide covering the personnel, resources, and procedures essential for restoring operations after a data loss or system failure. By preparing these guidelines in advance, SMBs can respond swiftly to restore systems and data, minimizing downtime, reducing financial impact, and avoiding potential penalties.

Choosing to forgo disaster recovery planning and creating a disaster recovery plan can significantly contribute to downtime, costs, penalties depending on your industry, and confusion during a cyber incident. Without a clear-cut guide, team members may impulsively respond before thinking about long-term consequences, redundancy may add to recovery time, and further disruption can occur, leaving clients without business-critical data for longer.

Why Use a Disaster Recovery Plan Template?

For MSPs, it's vital to have an individualized backup and recovery plan for each client to provide best-in-class BCDR execution following a data loss incident. The recovery plan must account for each client's specific business objectives, recovery point objectives (RPO), and recovery time objectives (RTO).

Creating an individualized plan for each client from scratch can be daunting, especially if you have clients that span different verticals. Many MSPs find value in using a disaster recovery plan template to guide their initial efforts and speed up the plan creation for each client. Working from a template…

- **Accelerates the development** of the disaster recovery plan.
- **Protects against common oversights** and gaps that often occur without planning.
- **Creates a standard structure** so all client records are aligned and easily executable.

Determining RPO and RTO Targets

When figures such as RPO and RTO are theoretical, client companies may be more willing to gamble. One way MSPs can successfully leverage RTO and RPO to put client's minds at ease is by attaching concrete numbers to the concepts. This lets customers quantify precisely what downtime will cost them in black and white.

Precise RTO and RPO figures will be dictated by a company's business continuity plan or business impact analysis (BIA). The continuity plan will be the basis of the design of the company's computer systems and infrastructure. The BIA should contain a risk analysis, which will be used in part to calculate RTO and RPO. ssThe BIA will outline the technologies, personnel, and facilities used in the event of a disaster and should include elements of financial loss, such as fees, fines, lost business revenue, and necessary overtime by IT personnel. Companies may also wish to include indirect losses, such as a loss of goodwill and reputation or increased customer churn.

It's not a simple process. The BIA may vary depending on the nature of the threat to the IT infrastructure. For example, the analysis of an extended power outage might look very different from predictions involving a ransomware attack. Calculations for applications will also vary depending on how critical they are. For instance, a client's HR database might be completely unharmed by days-long outages, but their financial transactions or online ordering system might need near real-time responses.

Once all these risks and scenarios have been defined and quantified, IT departments can analyze infrastructure assets and their corresponding tolerance for risk. They can then calculate RPO and RTO values and communicate them to the business's senior management team. To determine RTO, you can utilize Axcient's Direct-to-Cloud Recovery Time Objective Calculator.

How Do You Use a Recovery Plan Template?

Every business will have a DR plan unique to its company, location, and infrastructure. For example, a Florida-based company would find it valuable to include details about recovering after a hurricane. In contrast, a Canadian company would find it more beneficial to detail what to do if a blizzard knocks out power to its data center. Because the discrepancies between individual recovery plans can vary, it should be noted that no template, no matter how comprehensive, can provide a bulletproof plan for every company. When using a template, it's essential to alter it to provide for the unique elements and challenges of the specific business.

An Overview of Axcient's Disaster Recovery Plan Template

Below is an outline of a broad template that will provide a good foundation for MSPs to develop a disaster recovery plan for each client. It explains what should be covered in each section and offers common questions to ask yourself and your clients to ensure you capture the most comprehensive and accurate information. Any examples provided in the template are simply examples and are not intended to establish the requirements of a backup and recovery plan.

You can build your plan using the template below or download customizable templates to make it easier to update, amend, and brand.

> Download the DR Plan Technical Template
>
> Download the DR Plan SLA Template

Overview

The overview briefly introduces the disaster recovery plan and its intended purpose. Most plan overviews touch on how backup and recovery relate to data protection and cybersecurity and how those items impact the organization.

Example: *A backup and recovery plan is a critical data protection component. Any data loss due to a cyberattack, natural disaster, security breach, or human error can negatively impact business operations and contribute to financial losses. An effective contingency plan is crucial to <Company>.*

Purpose

This section documents why the plan exists. In most cases, the purpose will be to provide written documentation to guide the backup and recovery of critical data.

Example: *The purpose of this plan is to ensure <Company> can effectively and securely backup mission-critical data, systems, databases, and other technologies that impact normal business operations. The plan details the procedures for successful data recovery during a catastrophic data loss event.*

Scope

The scope outlines to whom the plan and policies outlined within it apply and the data and devices covered by the plan. If your plan does not include certain pieces of infrastructure, such as individual workstations or tablet PCs, make sure to detail those exclusions in the scope as well.

Example: *The scope of this plan applies to all employees at <Company>. This plan includes, but is not limited to, backup and recovery of file and print servers, mail servers, web servers, and domain controllers. This plan does not include the backup and recovery of personal devices or iPads.*

Risk Management Chart

The risk management chart provides an executive summary of the probability of a specific event and its impact and consequences on the business. Generally, these charts are done in table form and detail the following:

- Potential disaster
- Probability rating
- Impact rating
- Description of consequences

This type of risk planning can also help guide the creation of the rest of the recovery plan. Suppose the risk management chart reveals that a natural disaster is the most probable disaster with the highest impact. In that case, more time should be spent planning a detailed contingency plan for that scenario versus an event that is not as likely to happen and will have a lesser impact should it occur. Note that not all businesses choose to include a risk management chart in their backup and recovery plan. Your location and threats to the individual client will dictate the need for this chart in your documentation.

Inventory

Most disaster recovery plans will include an inventory of all the components that comprise the organization's IT infrastructure. This comprises all hardware, software, databases, network services, and other devices or networks contributing to business continuity. The inventory can come up front in the plan or be included as an appendix.

It's best practice to not only develop a complete inventory but also to establish tiered recovery options for each piece of infrastructure based on its importance to business operations. Creating this hierarchy enables the quick restoration of essential functions while deferring granular recovery of less critical data to a later point in time. Here are three tiers to help with categorizing and questions to consider when sorting devices and systems into these categories.

1. Mission Critical

One of the primary goals of any disaster recovery plan is to resume normal business operations as quickly as possible. Devices and systems will fall into the mission-critical tier if they are absolutely essential to maintaining business continuity. For many companies, communication infrastructure, including email, phones, and chat, is one of the first pieces of the infrastructure to be restored. To make sure you're including the correct pieces in this tier, consider the following:

- What devices and systems, if they go down, would cause a complete failure of business operations?
- What components or data will affect the entire system if they continue to be offline? Consider how reliant a system or data is on other systems or data.
- Which parts of the infrastructure are necessary for baseline business continuity?
- Are there any devices or systems that will cause another emergency if they are not immediately brought back online?

While building out the mission-critical inventory, always refer back to your RTO. Prioritize restoring the infrastructure that will allow the recovery process to meet those objectives.

2. Intermediary

Inventory in the intermediary tier includes devices and systems that, while necessary, will not wholly shut down the business. This tier will vary from business to business, so it's essential to let the client's business objectives guide what gets classified as intermediary.

3. Low Priority

The low-priority tier encompasses devices, systems, and networks that do not immediately impact business continuity. For most organizations, this includes individual user devices and other personal equipment.

- What devices can be replaced or offloaded for temporary use? (Many devices that can be virtualized can be considered low priority, as the VM allows the return to normal operations while the recovery process is still underway.)
- What devices, systems, or data can be offline, potentially for weeks, and not cause an impact on the business?

Contacts

One of the most critical pieces of successful contingency planning is knowing who is supposed to take what action and how to contact those people. To that end, a disaster recovery plan should include a directory of the following personnel.

- **Data Backup Team** – The team responsible for implementing the backup procedures listed below.
- **Disaster Recovery Team** – The team executing the recovery plan after a disaster.
- **Approved Vendors** - List of vendors that provide mission-critical services. This can include vendors such as a backup or BCDR provider.
- **Insurance and Regulatory Info** - A good recovery plan involves communicating with insurance and regulatory bodies. Having this info on file accelerates the communication process.

Backup Procedures

Regular data backup is one of the most critical pieces of a disaster recovery plan. Studies show that restoring from a backup is the quickest and most cost-effective way to recover data that has become corrupted or lost/deleted. Organizations that leverage backups can restore the majority of their data within a week at a fraction of the cost of those that do not.

Backup Plan:

The backup plan dictates precisely what will be backed up, how often, and by who. This plan is a critical part of the backup procedures, as it ensures that your MSP is poised to protect clients from the ramifications of data loss. Some questions to consider when formulating the backup plan include:

- **What's the client's RPO?** The most critical part of the backup plan is establishing the RTO, which is the maximum amount of time that can pass before an element of the business is considered outdated. Setting this objective requires knowing how often you must conduct backups to revert without intolerable impact on operations. Calculating RPO requires assessing how much data loss you can tolerate if a disaster occurs.

- **How often will backups occur?** The answer to the question should come directly from the RPO. The client's ability to tolerate data loss will drive backup schedules. It's also important to understand that not every business asset will be backed up on the same schedule - this will depend on how often information changes and how critical it is to business operations. For example, a website may only need to be backed up every few days, whereas a CRM may need backup every few minutes.

- **Are there any special events that require backup?** Think through if there are any situations or events that happen on occasion but are not often enough to dictate a regular backup. For instance, many companies require a backup before upgrading or modifying a server. Include any larger, important tasks here so they're not overlooked.

- **What will be backed up?** Refer back to the inventory taken earlier in this template. Ideally, all infrastructure that can be backed up should be backed up. Once again, this will depend on the client's appetite for the risk of data loss and the backup storage available to them. At the very minimum, prioritize mission-critical and intermediary inventory in your plan.

- **How will backups be conducted?** The backup plan should dictate exactly how backups are conducted. Remember to list any software used for backups, and if you are using physical backup media, such as tapes, include those in this section as well.

- **Who will conduct the backups?** If you completed your contact list in the step above, you should have a comprehensive record of all the parties involved in backups. For this section, you'll want to divide that list and dictate who is responsible for backing up which systems. For some companies, this is as broad as "the IT team," whereas other organizations will list the specific personnel responsible.

- **What's the process in the event of a backup failure?** Finally, the backup plan should also include the corrective procedure if a backup fails. A comprehensive outline of this process will include who to report the failure to, the timeframe in which the issue should be solved, the following steps after a backup failure, and who is responsible for those next steps.

Backup Types:

Once the backup plan is set, you'll need to dictate what types of backups are used for each procedure. If you're running multiple types of backups (think full backups vs. incremental backups), you'll want to state when and how often each backup type will be used.

Example: *<Company> uses two types of backups: 1) Full backups will be run each Friday at 6 PM EST. In the event of a holiday, the full backup should be run at the close of business the preceding business day. Full backups will also be run after the close of business on the last business day of the month. 2) Incremental backups will be run daily.*

If your client has different systems that require a different cadence of backups, note the level of granularity in this section.

Backup Storage & Security:

The final part of your backup procedures should lay out how backups will be stored, including retention policies and any relevant security details. Here, you'll want to outline whether you plan to use an on-premise appliance, a direct-to-cloud instance, or a hybrid solution incorporating both on-prem and cloud storage options. Find guidance on which option suits your clients in Choosing the Right Data Backup Solutions for Your MSP. Depending on the data backup solution implemented for the client, this section of the disaster recovery plan will vary. Here are a few questions you should consider for each backup type to ensure that you've covered all your bases:

On-Premise Backup

- **Where are the appliances physically stored?** Ensure that the physical location can accommodate the existing appliance (s) and allow for additional appliances if storage capabilities are expanded in the future. Also, ensure that the physical location supports the security and disaster measures outlined below.

- **What security measures must be implemented to protect the appliances?** These can include security alarms, locked cages or cabinets, controlled access by traditional methods such as lock and key or electronic access systems using swipe cards and other credentials, close-circuit security monitoring, and other security measures appropriate for the client's location and organizational needs.

- **What disaster-related measures must be implemented, and where are they located?** Consider fire alarms, fire suppression devices such as fire extinguishers, and power protection devices such as surge protectors, backup batteries, and generators.

Direct-to-Cloud Backup

- **What security standards must a cloud provider comply with?** This will vary by client, but common security standards include SOC 2, ISO, HIPAA, and GDPR.

- **Does your client require geographic redundancy?** Determine whether the sensitivity of the information being backed up dictates multiple cloud backups in separate geographic locations.

Hybrid Backup Solution

You'll need to consider the questions posed for each backup type above for a hybrid backup solution. There are also a few unique procedures that will need to be considered, including:

- **Should the cloud backup be a 1:1 redundancy of the appliance backup or vice versa?** Many MSPs using a hybrid backup solution choose to run duplicate backups on each system so that a secondary backup is always available should one system fail. However, this decision will depend on the client's needs.

- **If the cloud and appliance backups aren't duplicates of each other, what type of data should be stored on each?** Document what each type of backup should accomplish for the client.

- **Are there separate retention policies?** Determine whether the cloud and appliance should have the same retention policies or if one should have a longer policy for extra protection while freeing up space on the other backup system.

Restoring Lost Data

Once your backup procedures are in place, you'll want to outline how to respond to a data loss event. Due to the nature of the events, this plan will generally differ from a business continuity and disaster recovery plan (outlined below). This plan is for recovering data after a minor, non-malicious incident, such as accidental deletion or user error. Here are five questions to guide creating your data loss recovery plan:

1. Who will determine when and what was lost?
2. Who will determine what methods are used for restoration?
3. How will data be restored, and what backups will be used to restore?
4. Who will oversee restoration?
5. Who will determine if the restoration is complete?

Business Continuity and Disaster Recovery Plan

Your backup and recovery strategy should include a comprehensive BCDR plan in addition to a data loss recovery plan. A disaster recovery plan (DRP) is different. It provides procedures that enable organizations to recover if a significant disruptive event interferes with or stops business operations entirely. These types of events can include natural disasters and malicious cyberattacks, such as malware, DDoS, and ransomware. One of the main goals of disaster recovery procedures is to recover systems and information as quickly as possible. Limiting downtime is critical to avoiding intolerable consequences that can further affect the business. Below is an outline of what to include in the BCDR plan section of your disaster recovery plan template. For a more in-depth guide on creating a BCDR plan, refer to Axcient's Guide to Creating a Disaster Recovery Plan.

Disaster Recovery Team:

Some roles to consider include:

- Who determines when the disaster recovery plan should be implemented?
- Who is in charge of directing recovery operations?
- Who is in charge of communications? If this differs for internal vs. external comms, note that difference here.

Recovery Timeline/RTO:

RTO measures the time from when a disruptive event occurs to when the IT resources must be fully operational. Your disaster recovery plan should dictate any SLAs with your client around their expected recovery timeline.

To help clients determine their RTO, refer to our Direct-to-Cloud RTO Calculator.

Communications:

Clear communication is a vital part of a backup and recovery plan, as it can help reduce panic, maintain trust, and avoid reputational damage. A comprehensive communication plan will address the following audiences:

- **Internal:** An internal communication plan helps avoid panic and ensure organizational cohesion. Apprise all employees across the organization of the situation, potential impacts, and any actions they need to take
- **External:** External communication encompasses the strategy to inform stakeholders, customers, partners, and the media, if necessary.
- **Regulatory/Insurance:** Depending on the client's industry, disasters or breaches must be reported to relevant regulatory groups or insurance companies.

Maintaining Your Disaster Recovery Plan

Creating a comprehensive DR plan is only the first step. Regularly maintaining and updating the plan is necessary to ensure it remains up-to-date and ready for action. The plan must be maintained and updated regularly. To ensure that audits and updates are being done regularly, consider putting a review cycle into place. This could be every year, or a quarterly cadence might be more prudent for more sensitive or rapidly evolving industries. During these regular audits, you'll need to comprehensively review the entire plan and ensure that it aligns with the client's current environment and business operations.

In addition to regular updates, the plan should be updated each time a significant change is made to the business. This could include a shift in the leadership organization chart, a switch in BCDR vendors, or an updated backup schedule. Whether an update to the plan happens as part of the regular review process or is made ad hoc, keeping track of the revision is critical to ensuring that the most up-to-date plan is always referenced. The best practice would be to utilize document control software that keeps track of all revisions and documents that provide a reason for updating and codifies the review process. This type of stringent control is required in some industries (e.g., medical companies that need FDA approval) but is not necessary for others. Regardless of how document control is achieved, ensure that a log of the revision history and numbers is kept so there is no question about which version of the plan to use.

Once the plan has been revised, a straightforward process should control its distribution. As in previous steps of this template, identify who is in charge of the distribution, who needs to know about the revised plan, and how the plan will be distributed.

Supporting Your Disaster Recovery Plan with BCDR Solutions

Various BCDR solutions on the market make it easier for MSPs to support their clients. These platforms help minimize downtime, meet compliance standards, enhance data security, and enable MSPs to stay competitive. Finding the right disaster recovery provider will depend on the type of clients you serve, their business needs, and the business needs of your MSP.

Axcient x360Recover is the most comprehensive and cost-effective BCDR solution for MSPs and their SMBs. With just one solution and one vendor, MSPs can meet a range of client needs based on budget, environment, infrastructure, and compliance requirements. To learn more about Axcient's flexible deployment options, single sign-on platform, and proprietary technologies…

Schedule Your 1:1 Demo

Start Your Free 14-Day Trail

Get Your BCDR Quote

Get Done-For-You Disaster Recovery Plan Templates

Data loss can wreak havoc on clients and, in many cases, lead to the eventual shuttering of the business. A comprehensive disaster recovery plan is vital for today's businesses. As an MSP, you must protect a client's data via backups and be prepared to remediate data loss quickly. Use this broader template as a starting point in your mission to protect your clients against data loss, or download the already-done templates below and start customizing immediately.

> Download the DR Plan Technical Template
>
> Download the DR Plan SLA Template

About Axcient

Axcient is an award-winning leader in business continuity and disaster recovery for Managed Service Providers (MSPs). Axcient x360 provides one platform for MSPs to Protect Everything ™, and includes BCDR, Microsoft 365 and Google Workspace backup, and secure sync and share. Trusted by more than 5,400 MSP partners worldwide, Axcient protects business data and continuity in the event of security breaches, human error, and natural disasters.

Axcient

Axcient, 707 17th Street, Suite 3900, Denver, CO, 80202
Tel: 720-204-4500 | axcient.com