US SIGNAL

YOUR 12-POINT DR PLANNING TO-DO LIST

If you're considering implementing a disaster recovery (DR) plan, this "to-do" list* will help in making key decisions that will affect its structure and effectiveness.

Even if you already have a DR plan in place, you can use this checklist to help ensure you're covering the key elements of an effective DR strategy.

1 GAIN A SOLID UNDERSTANDING OF DR

Educate yourself on DR best practices and learn the differences between DR and business continuity (BC), replication and backup, and traditional and cloud-based DR options.

There are a variety of resources available, including a number at the **Department of Homeland Security's** web site and at the web site for the **Disaster Recovery Journal**.

COMPLETED

Y: N:

2 RESEARCH AND UNDERSTAND LAWS AND REGULATIONS REGARDING DR, PARTICULARLY THOSE SPECIFIC TO YOUR INDUSTRY

Seek professional advice from compliance experts. In many cases, they can also provide guidance on necessary certifications, third-party audit requirements and other information.

If you're considering outsourcing any portion of your DR efforts, work with vendors that have compliance experts of staff and that, themselves, are compliant and hold pertinent certifications.

COMPLETED

Y: N:

3 INVENTORY AND PRIORITIZE YOUR IT ASSETS

Inventory your IT assets. Take into account "shadow IT" that could have introduced essential data and applications without the knowledge of your IT department. Identify all application and system dependencies.

Determine which assets are most critical to your organization. Estimate how long your business could get by without access to them, if at all, and which would need to be recovered first following a disaster.

COMPLETED

Y: N:

4 CONDUCT A RISK ASSESSMENT

Examine the vulnerability of your IT assets to events that can cause downtime, such as cyber-attacks, internet outages, and natural disasters.

Consider the wide variety of factors that affect downtime, such as geographical location, weather patterns, and human error.

COMPLETED

Y: N:

5 CONDUCT A BUSINESS IMPACT ANALYSIS (BIA)

Determine the operational, financial and reputational effects to your business if any of your IT assets weren't available including, but not limited to, lost revenue, regulatory fines, and brand damage. Identify the resources required to maintain your business operations, if possible. Establish an order of priority for restoring business functions and related data or applications.

COMPLETED

Y: N:

6 DEFINE YOUR RECOVERY POINT OBJECTIVES (RPO)

Set recovery point objectives for each of your critical applications. RPO tells you how much time from the point of the outage you can afford to lose. Your RPO will determine the frequency with which you'll need to replicate data from your production site to a DR site.

COMPLETED

Y: N:

7 DEFINE YOUR RECOVERY TIME OBJECTIVE (RTO)

Your RTO establishes how quickly you need to have data or applications back up and available after a disaster. This will vary widely depending on the application and/or data and who uses it.

COMPLETED

Y: N:

8 REVIEW DR STRATEGIES

Evaluate different data backup, replication and recovery strategies.

Among the questions to ask:

+ Is traditional or cloud-based the way to go?
+ If traditional is the way to go, will tape backup work or is disk backup the better option?
+ Should you keep data backups on site or move them to an off-site facility?
+ If you go with off-site backup, do you want a cold, warm or hot site?
+ If you're leaning towards cloud-based DR, is a public or private cloud environment appropriate?
+ Will the cloud environment meet any compliance requirements you have?
+ Will the cloud environment provide the level of security you require?
+ If you have both physical and virtual servers, can your physical applications be recovered in a cloud DR environment?

COMPLETED

Y: N:

9 DETERMINE IF YOU SHOULD MANAGE YOUR DR PLAN INTERNALLY OR OUTSOURCE SOME OR ALL OF IT

Review your internal staff resources. Do they have the time and expertise to devote to managing a DR plan, maintaining runbooks, keeping pace with changing technologies etc?

Do you have the budget and other resources to cover the purchase, maintenance, and management of the necessary infrastructure and other essential components? Would it make sense to trade CapEx for OpEx by going with an outsourced, managed DR service?

COMPLETED

Y: N:

10 BUILD YOUR DR TEAM

Even if you outsource some or all of your DR plan, you'll need an internal team to handle various aspects of your DR efforts. Assign roles and responsibilities.

If you're outsourcing, make sure you have key contacts on your side and the vendor side identified and regular communication between everyone in place.

COMPLETED

Y: N:

11 BUILD OUT YOUR DR PLAN BEYOND RESTORATION AND RECOVERY OF IT ASSETS

Your DR plan isn't just about your IT assets. It should also detail:

+ How your employees, management team, and your DR team will communicate with each other.
+ Your disaster response procedures, including how you'll report a disaster incident to stakeholders.

COMPLETED

Y: N:

12 TEST AND UPDATE YOUR DR PLAN

A DR plan doesn't benefit your organization if it doesn't perform as expected. Develop and implement regular testing procedures. Tests should be conducted at least annually, the results evaluated, and plan updates made as needed.

If you're outsourcing your DR, make sure the vendor provides the necessary testing and updates.

COMPLETED

Y: N:

YOUR NEXT STEPS

To learn more about developing a new DR plan or evaluating your existing one, contact US Signal. Our DR specialists can help you assess your current DR strategy and/or requirements. And if you're interested in a cloud-based DR plan, they can architect one best suited to your organization's needs.

866.274.4625 / info@ussignal.com

NOTES

**This checklist is for informational purposes and is not intended to use as a DR plan. Depending on your organization's business requirements, needs and other variables, there may be other factors to consider when developing and implementing a DR plan.*