tierpoint

# 13 Things to Include in Your Disaster Recovery Plan Checklist

Disasters can strike at any time and can have a devastating impact on businesses, causing significant downtime and financial loss. In fact, over **60%** of failures result in a total loss of at least **$100,000**.

**>60%**
**of outages**
*equals*
**$100k**
**lost***

## Having a well-planned and well-executed disaster recovery plan checklist is essential to ensuring that your business:

- Follows steps to protect data and operations
- Quickly recovers from a disaster
- Resumes normal operations ASAP

## Your Sample DR Plan Checklist

The checklist below is meant to serve as a tool to help ensure your DR plan is comprehensive, protects critical data, and maintains business continuity with minimal downtime. Keep in mind that specific items included within your checklist may vary due to the needs and risks of your organization.

☐ **1. Set RTO* and RPO* Targets**
Determine the maximum RTO and RPO for each system. It's important to set realistic targets that are acceptable and achievable with your current infrastructure.

☐ **2. Identify Critical Systems and Data**
Make a list that includes all of the systems, data, and applications that are critical to your organization's operations. i.e. identify the minimum level of system and data availability required to support BizOps.

☐ **3. Define Backup and Recovery Procedures**
Based on the RTO and RPO targets, plan and implement backup and recovery solutions that meet your needs. This may involve investing in backup and DR solutions like cloud backup or data replication.

☐ **4. Incident and Response Management**
Create and write down procedures for responding to and managing potential incidents, as well as identifying the individuals responsible for coordinating each response.

☐ **5. Disaster Recovery Team and Roles**
Determine who within your organization should be on the DR team and clearly define their role and responsibilities so they're prepared for each type of disaster.

☐ **6. Communication and Awareness Training**
Provide information about the DR plan to employees, define their roles in its implementation, and offer effective awareness training. Doing so will not only inform, but also may help uncover plan deficiencies.

☐ **7. Develop a Crisis Communication Plan**
Create a crisis communication plan that outlines how to communicate with, and who communicates to, employees, customers, partners, press, and other stakeholders in the event of a disaster.

☐ **8. Make Alternative Site Arrangements**
Identify and secure alternate locations for critical systems and data during a disaster, i.e. utilize cloud vs on-premises or a 3rd party data center. Be sure to consider location, accessibility, infrastructure, and compliance.

☐ **9. Plan for Failback**
Always plan for how to move operations from a temporary site back to its primary site. Without a failback plan, your team may encounter avoidable errors, crucial data loss, or even major delays.

☐ **10. Monitor and Document the Failback Process**
Watch the failback process and keep careful notes to ensure that it runs smoothly, and any systems, applications, and infrastructure are properly restored after failback has been completed and tested.

☐ **11. Supplier and Vendor Management**
Ensure that key supplier and vendor partnerships also include clearly defined DR procedures. These procedures should address interdependencies plus monitoring and testing to minimize downtime.

☐ **12. Test and Validate the Disaster Recovery Plan**
Prevention and preparation are key to ensuring full recovery after a disruption. Regularly test and validate your plan to ensure it meets RTO/RPO targets and compliance requirements.

☐ **13. Continuously Monitor and Update the Plan**
In addition to scheduling routine tests, it's mission-critical to review and update your organization's DR plan on an ongoing basis to make sure it stays rock solid, especially as new security threats take form.

## Get Expert Disaster Recovery Planning and Protect Your Data with TierPoint

Developing and testing a strong DR plan can be difficult, not to mention stressful. Leaving out one crucial piece or a potential scenario could hinder your business continuity plans, hurt your brand reputation, and lead to financial loss.

At TierPoint, our DRaaS® and BaaS® offerings, among others, can help you build and facilitate a DR plan that maintains resiliency for your mission-critical data, operations, applications, and overall IT infrastructure.

**Contact us today: www.tierpoint.com/contact-us**

tierpoint

*Stat source: Uptime Institute's 2022 Outage Analysis
*RTO = Recovery Time Objective (maximum length of time to restore to normal operations)
*RPO = Recovery Point Objective (maximum amount of data loss you can accept from point of last backup)
*DRaaS = Disaster Recovery as a Service
*BaaS = Backup as a service