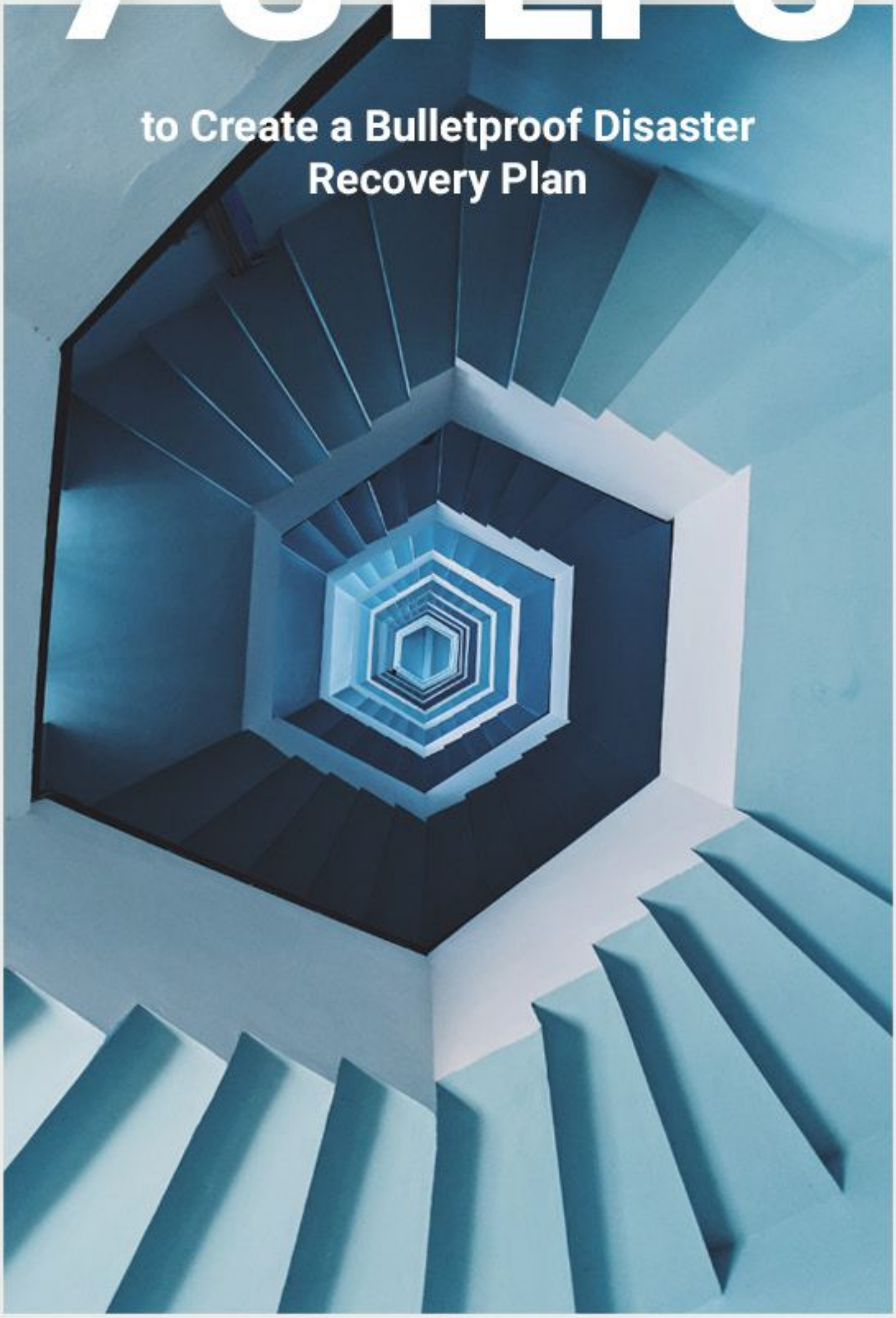
7 STEPS

to Create a Bulletproof Disaster Recovery Plan



Quorum®

The Leader in Disaster Recovery

Visit our website to learn why Quorum is the world leader in HA and DR solutions.

Few documents are more important to an IT department than a thorough disaster recovery (DR) plan.

When an emergency situation strikes, it's important to know *exactly* what needs to be done, how to do it, and who needs to be involved. A good disaster recovery plan includes all of these details and more.

Here are the 7 critical steps to creating a disaster recovery plan so you can ensure that your organization is protected against a worst-case scenario.

Conduct a thorough IT risk assessment

A comprehensive disaster recovery plan starts with cataloging all of your vulnerabilities that could lead to a potential DR scenario. Central to this process is identifying all critical applications and servers that need to be backed up.

Be thorough, exclude nothing and don't assume that you know what is best for your users. Make sure to include ancillary systems like domain servers, as well as other network equipment, circuits and locations.

This first step is critical as it will determine the necessary scope of your DR plan.

02

Complete a business impact analysis

Completing a business impact analysis is an important step in determining the recovery objectives and performance requirements for your DR system.

This is where you define key targets like recovery time objective (RTO) and recovery point objective (RPO) — two important but often misunderstood terms.

Your RTO refers to the maximum time a server, application or system can be down before it results in unacceptable damage to the business.

Your RPO refers to the maximum acceptable age of the backup files that are to be used during a disaster recovery incident. This number tells you how often your data must be backed up.

For instance, an RPO of 60 minutes means that for your business to avoid unacceptable losses, your DR system must recover data from no more than 60 minutes in the past. Therefore, your system must create automatic backups at least once per hour.

RTO: The maximum time a server, application, or system can be down before it results in unacceptable damage to the business.

RPO: The maximum acceptable age of the backup files that are to be used during a disaster recovery incident. This number tells you how often your data must be backed up.

When conducting your business impact analysis, it's a must to bring executives and other relevant management into the process (alongside technical experts) to ensure that you're prioritizing the right key elements, protecting the most important business objectives and striking a balance between risk mitigation and practicality.

03 Clearly define roles for your IT specialists

In an emergency, it is critical for everyone to know their role in advance. Once a DR incident begins, there is no time for deciding who is doing what.

When defining everyone's roles, which can and should go beyond operational IT recovery (ex. Communications, Insurance/Finance, etc.), make sure you answer the following questions:

- Who is the **one person** responsible for managing the recovery process? How do I contact them (ex. call tree)?
- Are certain members of your IT team more knowledgeable, experienced or adept at responding to certain types of security threats or service/system outages? Is there a way to delegate responsibility that maximizes your team's individual competencies?
- Who are the backups for each critical role in case the primary person is temporarily unavailable?
- Does your DR training loop in everyone who could conceivably play a role — even those who are not on the "A-Team"?

04 Catalog the exact steps to take in a DR incident

There are many different scenarios that can lead to a DR incident. Include clear playbooks with UAT testing steps that have been confirmed with business unit leaders for the most common security breach scenarios (malware, DDoS, phishing, etc.), as well as non-security related issues like single server and site failures.

Regularly updating your plan is as critical as creating it. Your plan should be revisited and updated every time you test your DR system, change infrastructure and/or key personnel, any time an employee involved in the plan leaves the organization or a new employee is hired who will have a roll in the plan going forward.

Make sure to clearly describe what events trigger an escalation to an IT manager, as well as what evidence needs to be gathered when a potential security threat is detected.

05

Establish a regular testing schedule

Testing used to be cumbersome and require unacceptable downtime. Modern technology has changed that, making it easy to perform realistic tests with little to no disruption to your business function.

Businesses in different verticals will have different best practices when it comes to test schedules. However, a good rule of thumb is to do a partial test monthly and a full test (including user acceptance testing (UAT)) at least once per year.

When you run a DR test, observe and record the following:

- How long did recovery take compared to the expectations from the business analysis?
- What data and/or workloads proved challenging to recover?
- If running a full test (including UAT): were all applications and related software returned to the exact state expected?
- Was the recovery process feasible for IT staff operating under stress with reduced tools?
- Would successful recovery be realistic if critical IT staff were not present?
- How would parallel recoveries amplify the challenges?

These questions will help you understand vulnerabilities that would continue to be invisible without performing a thorough analysis. They will also inform your choice of disaster recovery solutions and help you further refine and improve your DR plan.

06

Use test results to update DR plan

Your DR tests (especially full system tests) can do much more than simply validate that your DR system is functional. By asking the right questions, you can use the results of your tests to create an even better, more comprehensive and more bulletproof DR plan.

Ask yourself questions like:

- What vulnerabilities or potential issues did you uncover?
- What parts of the process (including software and other DR solutions) could be improved to make your DR process faster, more reliable, more efficient, or easier to perform?

Use these insights to explore ways to improve your system/process and to update your existing DR plan.

07 Review potential DR solutions based on recovery objectives and requirements

Now that you've created a comprehensive DR plan, it's time to evaluate whether you have the ideal disaster recovery solution in place.

Put simply, the right DR solution for your business is the one that best supports your objectives as outlined in your DR plan.

The right DR solution for your business is the one that best supports your objectives.

Ask yourself the following questions when evaluating your current solution, as well as alternative solutions on the market:

- How fast can recovery be completed?
- Does the solution meet or exceed our key metrics like RTO and RPO as outlined in the DR plan or business analysis?
- How easy is it to operate? Could a new IT hire reliably complete the recovery process while under pressure?
- How secure is the solution? Is it fully air gapped? How easy is it to manage access privileges?
- How reliable is the solution? Can it be counted on to perform in the full spectrum of potential emergency situations (from natural disasters to security breaches like ransomware)?

Quorum: The Leader in Disaster Recovery

Quorum provides the fastest, most reliable, and easiest-to-use high availability and disaster recovery systems on the market. Our industry-leading technology is built to deliver the ultimate in flexibility, performance and value. With Quorum, you no longer have to choose between cloud vs. local or cost vs. performance. **Visit our website** to learn why Quorum is the world leader in HA and DR solutions.

Contact Quorum Phone: 877-997-8678 | Email: ussales@quorum.com

Quorum®