6 Steps to Planning Disaster Recovery

Jim Hall

In the simplest definition: Disaster Recovery is what you do to recover your system from a disaster or outage. Business Continuity is what you do to keep conducting business while others recover the system.

When we talk about disaster recovery, most people immediately think of the “smoking hole in the ground” scenario. They imagine examples where the data center building is engulfed in an inferno or demolished by a tornado. In fact, disasters can be large or small.

In planning your response, consider the “small” disasters that can be just as devastating as a data center loss. Examples include a database administrator not checking the status of a backup before deleting a database to upgrade the database software. Or a water leak from an overhead sprinkler system that damages several racks of systems in a data center. Or construction workers who accidentally cut into the only fiber data connection for the data center.

What elements should you include in your next disaster recovery plan? The specifics may differ depending on the systems involved, but at a high level you will want to include these topics:

1. Identify critical people and vendors.

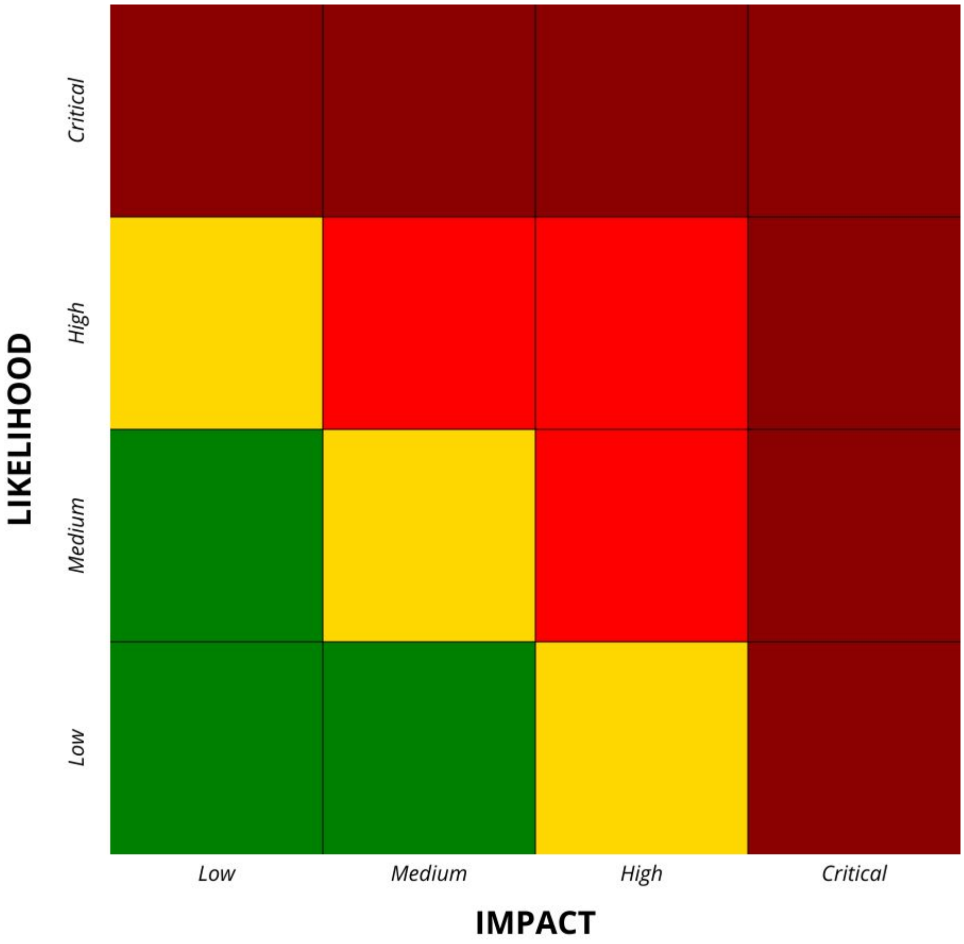
In most instances, disaster recovery is performed by the IT team, and business continuity is the responsibility of business units. But depending on the application, note that the players for these may overlap.

In a disaster, you will need to immediately reach out to technology folks to respond to the disaster, internal partners to keep the business running, and external vendors to help you get back to business quickly. Your next disaster may not be conveniently timed to occur during working hours. Make sure you have copies of contact information available off-site.

2. Identify critical systems and applications.

Conduct a risk analysis or other prioritization exercise to understand which systems are truly critical to your business. Create disaster recovery plans for these systems first. For example, most organizations can let development or test systems wait a few days while you restore production systems.

One way to prioritize systems and applications is to break it up into components: the likelihood of a failure, and the business impact of the failure. The combination of these components determines the criticality of the overall system.



3. Are your RTO and RPO realistic and achievable?

How quickly can you recover a system, and how old will your data be when you get it back up? These address two important factors in disaster recovery planning. RTO (Recovery Time Objective) is how long it will take to recover your system, and RPO (Recovery Point Objective) describes the age of the data that you can recover.

4. Design for redundancy and failover.

As you create a disaster recovery plan for an application, look closely at the systems it connects to. What inter-dependencies exist? How does your application rely on other systems and applications?

Where possible, create an architecture that remains flexible in the face of an outage. In one example, you might run production systems from two different data centers. But as you design failover into your architecture, look for single points of failure and find ways to address them.

5. What is your upstream's DR plan?

Many organizations now outsource applications, and leverage Cloud and vendor-hosted systems. While this simplifies your IT, it means the Cloud and other outsourced vendors become even more critical to your operations.

Be mindful not to be lulled into a sense of security when outsourcing applications and services. Just because you have outsourced part of your systems to a vendor or other upstream provider doesn't mean you can ignore disaster recovery planning for those systems. Discuss disaster recovery plans with your upstream vendor to understand how they will bring your applications and data back online in the face of a disaster. And review business continuity with your internal partners to ensure the business can continue running if the vendor's site is down.

6. How do you go back to normal?

It's tempting to focus only on the actual recovery portion of a disaster recovery plan. For example, your plan may require moving production to a test server. But you can't run production on the secondary system forever. Having recovered on the test system, how do you plan to go back to a normal state?

Take this opportunity to review processes and procedures in your own organization. What does your Disaster Recovery plan look like? Do you have one? Document your response and review your plans with others in your business line. Ensure everyone in the organization know how to bring systems back online in the face of failure, and how to continue business operations in the face of an outage. If you can do both, you will set yourself for success.