What Is Disaster Recovery?

Disaster recovery is an organization's method of regaining access and functionality to its IT infrastructure after events like a natural disaster, cyber attack, or even business disruptions related to the COVID-19 pandemic. A variety of disaster recovery (DR) methods can be part of a disaster recovery plan. DR is one aspect of business continuity.

How Does Disaster Recovery Work?

Disaster recovery relies upon the replication of data and computer processing in an off-premises location not affected by the disaster. When servers go down because of a natural disaster, equipment failure or cyber attack, a business needs to recover lost data from a second location where the data is backed up. Ideally, an organization can transfer its computer processing to that remote location as well in order to continue operations.

5 Top Elements of an Effective Disaster Recovery Plan

- **Disaster recovery team:** This assigned group of specialists will be responsible for creating, implementing and managing the disaster recovery plan. This plan should define each team member's role and responsibilities. In the event of a disaster, the recovery team should know how to communicate with each other, employees, vendors, and customers.
- **Risk evaluation:** Assess potential hazards that put your organization at risk. Depending on the type of event, strategize what measures and resources will be needed to resume business. For example, in the event of a cyber attack, what data protection measures will the recovery team have in place to respond?
- **Business-critical asset identification:** A good disaster recovery plan includes documentation of which systems, applications, data, and other resources are most critical for business continuity, as well as the necessary steps to recover data.
- **Backups:** Determine what needs backup (or to be relocated), who should perform backups, and how backups will be implemented. Include a recovery point objective (RPO) that states the frequency of backups and a recovery time objective (RTO) that defines the maximum amount of downtime allowable after a disaster. These metrics create limits to guide

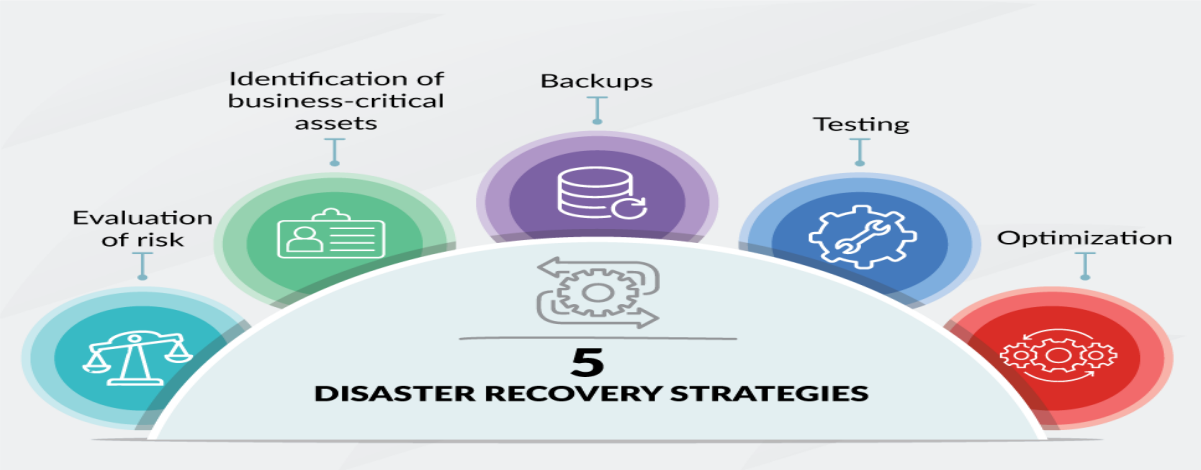
the choice of IT strategy, processes and procedures that make up an organization's disaster recovery plan. The amount of downtime an organization can handle and how frequently the organization backs up its data will inform the disaster recovery strategy.

- **Testing and optimization:** The recovery team should continually test and update its strategy to address ever-evolving threats and business needs. By continually ensuring that a company is ready to face the worst-case scenarios in disaster situations, it can successfully navigate such challenges. In planning how to respond to a cyber attack, for example, it's important that organizations continually test and optimize their security and data protection strategies and have protective measures in place to detect potential security breaches.

How to Build a Disaster Recovery Team

Whether creating a disaster recovery strategy from scratch or improving an existing plan, assembling the right collaborative team of experts is a critical first step. It starts with tapping IT specialists and other key individuals to provide leadership over the following key areas in the event of a disaster:

- **Crisis management**: This leadership role commences recovery plans, coordinates efforts throughout the recovery process, and resolves problems or delays that emerge.
- **Business continuity**: The expert overseeing this ensures that the recovery plan aligns with the company's business needs, based on the business impact analysis.
- **Impact assessment and recovery**: The team responsible for this area of recovery has technical expertise in IT infrastructure including servers, storage, databases and networks.
- **IT applications**: This role monitors which application activities should be implemented based on a restorative plan. Tasks include application integrations, application settings and configuration, and data consistency.



What Are the Types of Disaster Recovery?

Back-up: This is the simplest type of disaster recovery and entails storing data off site or on a removable drive. However, just backing up data provides only minimal business continuity help, as the IT infrastructure itself is not backed up.

Cold Site: In this type of disaster recovery, an organization sets up a basic infrastructure in a second, rarely used facility that provides a place for employees to work after a natural disaster or fire. It can help with business continuity because business operations can continue, but it does not provide a way to protect or recover important data, so a cold site must be combined with other methods of disaster recovery.

Hot Site: A hot site maintains up-to-date copies of data at all times. Hot sites are time-consuming to set up and more expensive than cold sites, but they dramatically reduce down time.

Disaster Recovery as a Service (DRaaS): In the event of a disaster or ransomware attack, a DRaaS provider moves an organization's computer processing to its own cloud infrastructure, allowing a business to continue operations seamlessly from the vendor's location, even if an organization's servers are down. DRaaS plans are available through either subscription or pay-per-use models. There are pros and cons to choosing a local DRaaS provider: latency will be lower after transferring to DRaaS servers that are closer to an

organization's location, but in the event of a widespread natural disaster, a DRaaS that is nearby may be affected by the same disaster.

Back Up as a Service: Similar to backing up data at a remote location, with Back Up as a Service, a third party provider backs up an organization's data, but not its IT infrastructure.

Datacenter disaster recovery: The physical elements of a data center can protect data and contribute to faster disaster recovery in certain types of disasters. For instance, fire suppression tools will help data and computer equipment survive a fire. A backup power source will help businesses sail through power outages without grinding operations to a halt. Of course, none of these physical disaster recovery tools will help in the event of a cyber attack.

Virtualization: Organizations can back up certain operations and data or even a working replica of an organization's entire computing environment on off-site virtual machines that are unaffected by physical disasters. Using virtualization as part of a disaster recovery plan also allows businesses to automate some disaster recovery processes, bringing everything back online faster. For virtualization to be an effective disaster recovery tool, frequent transfer of data and workloads is essential, as is good communication within the IT team about how many virtual machines are operating within an organization.

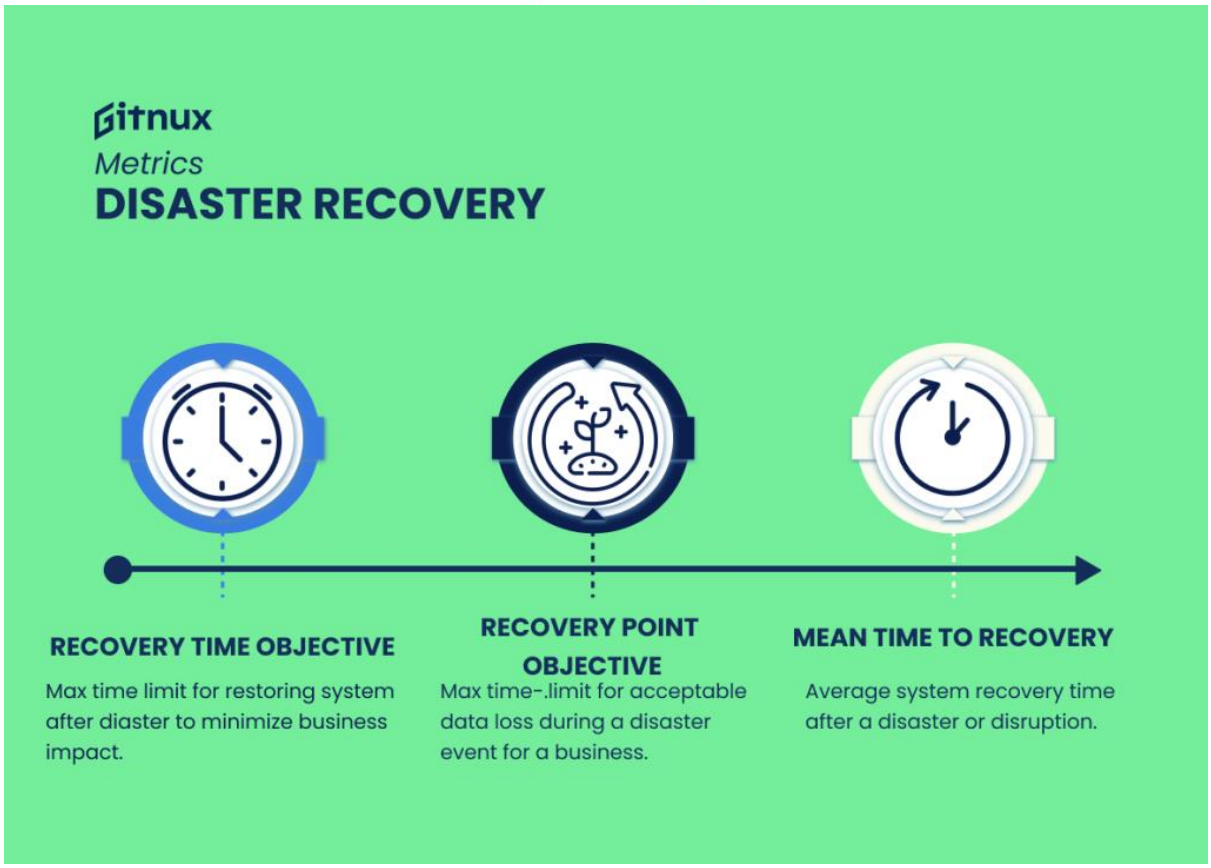
Point-in-time copies: Point-in-time copies, also known as point-in-time snapshots, make a copy of the entire database at a given time. Data can be restored from this back-up, but only if the copy is stored off site or on a virtual machine that is unaffected by the disaster.

Instant recovery: Instant recovery is similar to point-in-time copies, except that instead of copying a database, instant recovery takes a snapshot of an entire virtual machine

What Are the Benefits of Disaster Recovery Software?

- **Cost savings:** Planning for potential disruptive events can save businesses hundreds of thousands of dollars and even mean the difference between a company surviving a natural disaster or folding.

- **Faster recovery:** Depending on the disaster recovery strategy and the types of disaster recovery tools used, businesses can get up and running much faster after a disaster, or even continue operations as if nothing had happened.


Gitnux
Metrics
DISASTER RECOVERY
RECOVERY TIME OBJECTIVE
Max time limit for restoring system after diaster to minimize business impact.
RECOVERY POINT OBJECTIVE
Max time-.limit for acceptable data loss during a disaster event for a business.
MEAN TIME TO RECOVERY
Average system recovery time after a disaster or disruption.

How to calculate maximum allowable downtime?

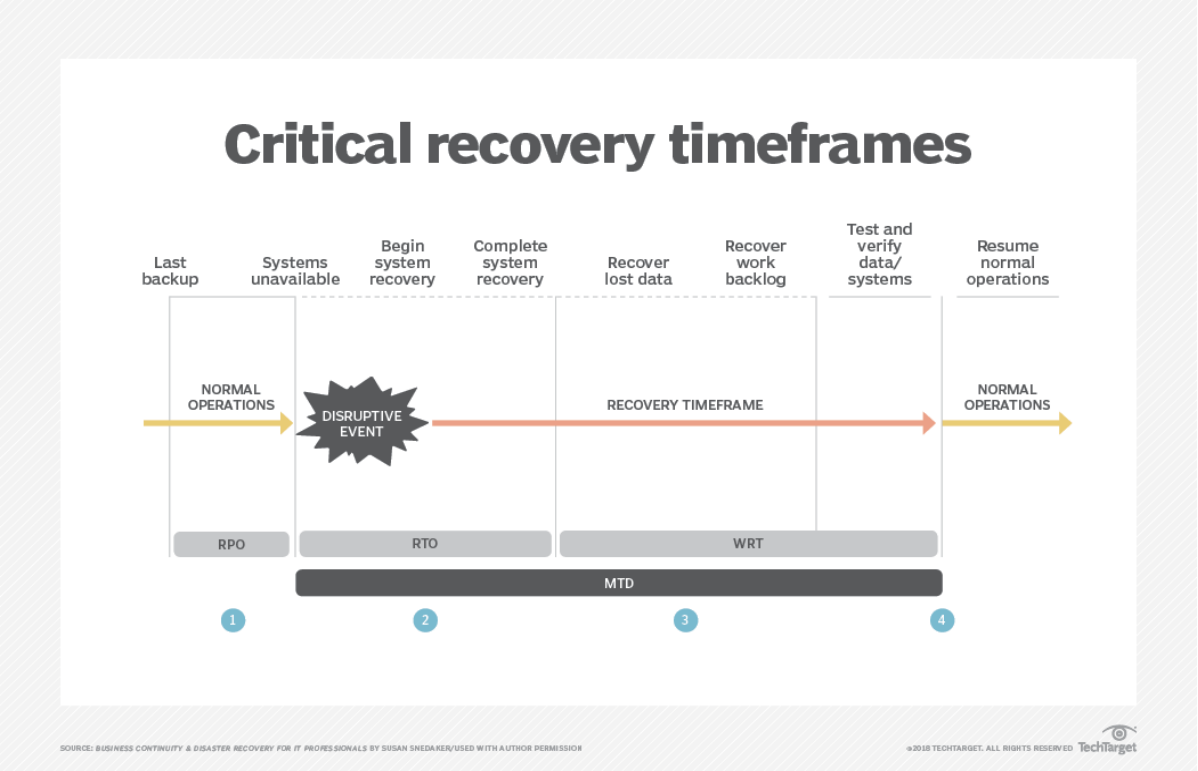
Maximum allowable downtime, also referred to as maximum tolerable downtime (MTD), is the absolute longest amount of downtime an organization can tolerate before facing serious repercussions. These can include loss of business or reputational damage.

Calculate maximum allowable downtime:

Maximum allowable downtime = RTO + WRT

For example, if a critical business process has a three-day maximum allowable downtime, the RTO for systems, networks and data might be one day. This is the

time the organization needs to recover technology. The remaining two days are for work recovery.



Point 1: Recovery point objective (RPO). The maximum sustainable data loss based on backup schedules, data needs and system availability.

Once the disruption occurs, the organization launches incident response activities. If it cannot bring the disruption under control quickly, DR teams launch data or system disaster recovery activities to return operations to normal as quickly as possible.

Point 2: Recovery time objective. This is the amount of time an organization needs to bring critical systems back online. This is where disaster recovery activities typically occur.

Point 3: Work recovery time. Once mission-critical systems and data resources are recovered and again operational, this is the time needed to get back to business-as-usual operating conditions.

WRT includes:

- Recovery of lost data (based on RPO);
- reentry of data from work backlogs, such as those manually generated during the outage;
- return of employees to their work areas;
- reactivation of systems, workstations, laptops, communications and other tools; and
- reengagement of linkages across operating units that make the company operate normally.

Point 4: At this point in time, the organization is back to business as usual, and it is time to review what happened during the event. DR teams must note what worked, what didn't work, what changes need to be made and the next steps going forward to deal with future disruptions.