

# DISASTER RECOVERY

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **S.No.** | **Title** | **Page No.** |
| 1 | What is Disaster Recovery? | 2 |
| 2 | Why is Disaster Recovery Important? | 3-4 |
| 3 | Disaster Recovery Types | 4-5 |
| 4 | How Disaster Recovery Works? | 5-6 |
| 5 | Examples of Disaster Recovery | 6 |
| 6 | What Is a Disaster Recovery Plan? | 7 |
| 7 | Elements of a DR Plan | 8 |
| 8 | How to Create a Disaster Recovery Plan? | 9-10 |
| 9 | Forming a Strong DR Team | 11 |

# DISASTER RECOVERY

A sound disaster recovery (DR) strategy helps companies recover from emergency scenarios, whether of natural, accidental, or malicious origin. By ensuring the company can quickly resume IT operations in times of crisis, DR helps prevent revenue losses, unhappy customers, and brand damage.

This is an introduction to disaster recovery and the ways security-aware companies prepare for emergencies. We explain all major DR concepts, look at different restoration strategies, and outline all you need to cover to create an effective disaster recovery plan.



## What is Disaster Recovery?

Disaster recovery (DR) is a set of procedures, policies, and processes that dictate how a company responds to disruptive events and incidents. Companies typically structure their DR strategy into a formal document that provides teams with detailed instructions for responding to disasters.

The goal of DR is to ensure a business can either continue to operate or quickly resume IT operations if there is a natural or human-induced incident. Common disaster scenarios are:

* + Natural hazards like tsunamis, earthquakes, floods, or hurricanes.
  + Failure of equipment (power outages, hard disk failures, physical damage, etc.).
  + Accidental human errors, such as unintentional erasure of data or the loss of a BYOD device.
  + Fire outbreaks.
  + Industrial accidents.
  + A malicious insider sabotaging a system.
  + Bomb threats.
  + A cyber-attack coming from outside the organization (DDoS, SQL injections, ransomware attacks, etc.).
  + A data breach.

Companies often combine disaster recovery and business continuity planning into a single initiative (BCDR). However, despite some overlap, there is a clear distinction between BC and DR:

* + Business continuity is a proactive set of practices that minimize risk and ensure the business can continue to deliver services without disruptions.
  + A disaster recovery plan is a reactive process that outlines specific steps a company must take to resume IT operations in case of a disaster.

## Why is Disaster Recovery Important?

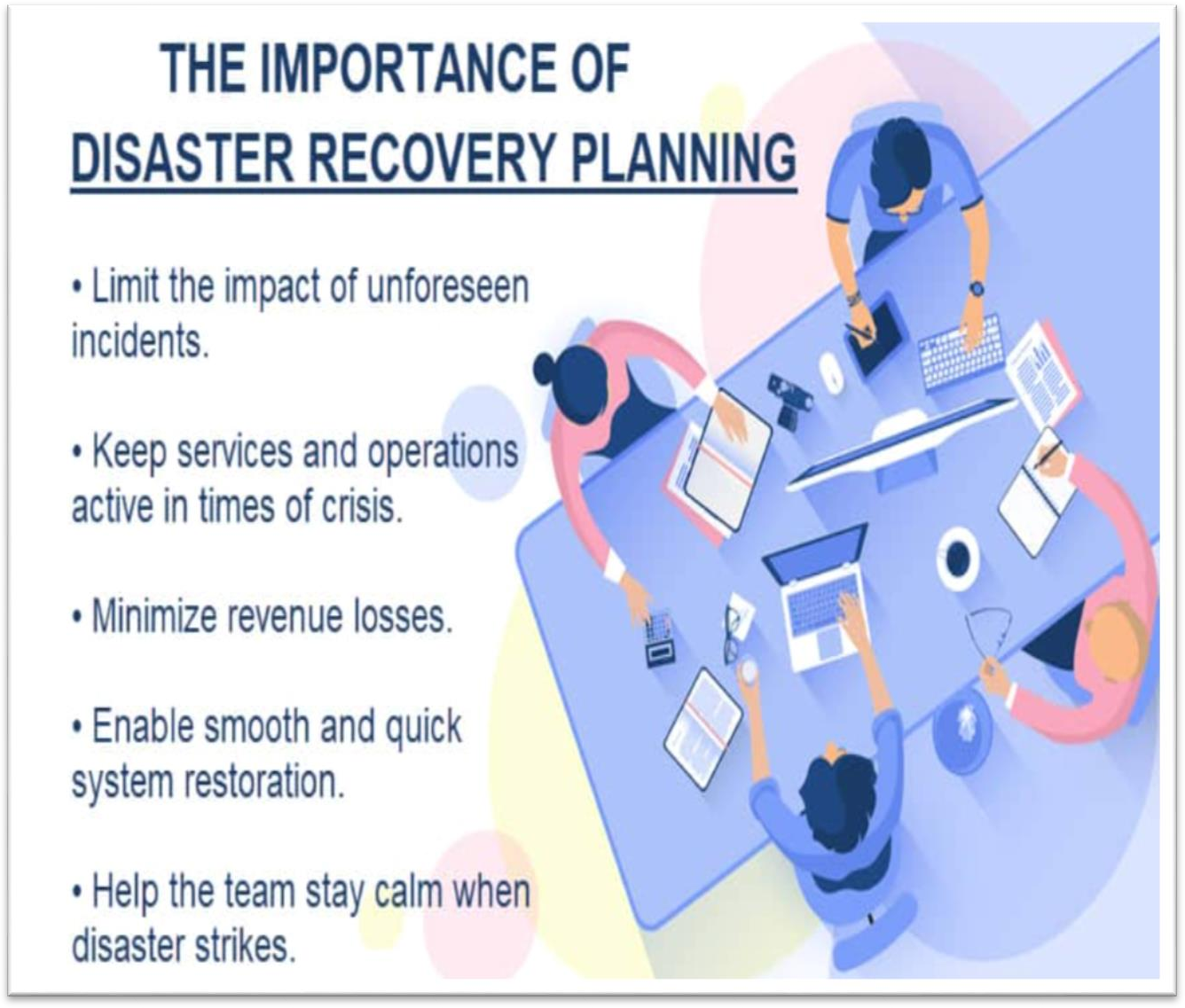
Disaster recovery is vital as it enables a company to:

* + Predict and prevent avoidable incidents.
  + Respond to and recover from unavoidable events.

When disaster strikes, a recovery plan reduces the damage and helps the team respond to the problem correctly. As a result, DR enables the following benefits during and after an emergency:

* + **Cost savings:** Preparing for a disruptive event can save hundreds of thousands of dollars in damages (safer equipment, better data protection, less legal consequences, etc.).
  + **Fast recovery:** A business can restart mission-critical services faster with a DR than without a reaction plan.
  + **No service interruptions:** A DR plan ensure services continue to run as if the disaster did not happen.
  + **Lower team stress:** Disaster preparation lowers the pressure on employees by giving the team a clear plan of action in case of an emergency.

Some businesses require disaster recovery plans to meet compliance regulations. Companies operating in financial, healthcare, and government sectors are typically legally obliged to have some form of DR readiness.



## Disaster Recovery Types

Companies can choose from a variety of DR types and methods to form an effective recovery strategy. The kind of disaster recovery you set up depends on your:

* + IT environment and its unique needs.
  + What assets require protection (digital and physical).
  + Industry risk levels.
  + The preferred methods of backup and recovery.
  + Overall budget.

Here are the most common types of disaster recovery:

* + **Data center disaster recovery:** This DR type ensures the company has a failover site at a secondary data center or a [colocation](https://phoenixnap.com/blog/what-is-colocation-hosting) facility. This plan should also include measures for recovering the primary [data center](https://phoenixnap.com/blog/data-center-tiers-classification) (e.g., fire suppression tools or

backup [power sources](https://phoenixnap.com/blog/data-center-power)).

* + **Cloud disaster recovery:** Instead of setting up a secondary facility, you can

use [cloud disaster recovery](https://phoenixnap.com/blog/cloud-disaster-recovery) to set up automatic workload failover to a cloud in the event of a disruption. This type of DR can include anything from reserve [cloud](https://phoenixnap.com/blog/what-is-cloud-computing)

[computing](https://phoenixnap.com/blog/what-is-cloud-computing) resources to a standby [virtual data center (VDC)](https://phoenixnap.com/blog/what-is-virtual-data-center).

* + **Network disaster recovery:** This DR strategy is a plan for restoring network functionality during a disaster. This plan typically involves access to backup sites and data.
  + **Virtualized disaster recovery:** [Virtualization](https://phoenixnap.com/kb/what-is-server-virtualization) allows you to replicate small- footprint workloads in an alternate location or the cloud.
  + **Disaster-recovery-as-a-service (DRaaS):** [DRaaS](https://phoenixnap.com/disaster-recovery-as-a-service-draas) is a service-based version of cloud disaster recovery. If there is an emergency, the DRaaS provider moves all computer processing to its cloud infrastructure and enables you to continue operations.

Depending on the scope and complexity of your IT setup, you may require multiple (or even all) of the recovery types listed above.

## How Disaster Recovery Works

Disaster recovery relies on replicating data and computing processes in an off-premises location unaffected by the ongoing incident. These locations can be either physical or virtual and fall into one of three categories:

* + **Cold sites:** A cold site is a secondary facility with power and networking capabilities. These sites do not include data storage, so setting them up in the event of a disaster is time-consuming and prone to mistakes.
  + **Warm sites:** A warm site contains all the elements of a cold location in addition to data storage hardware. These sites are ready to go if disaster strikes, but the team still needs to transport current data.
  + **Hot sites:** A hot site is a fully operational backup site with up-to-date mirrors of all critical data. These locations are time-consuming to set up and maintain but ensure little to no downtime in an emergency.

The type of site a company sets up depends on the complexity of the IT environment and the allocated budget. As cold sites are cheap to set up and hot locations are highly complex and costly, most companies opt for a warm backup.

## Examples of Disaster Recovery

Recovery strategies vary in complexity depending on the type of incident and the value of assets you are trying to protect. Here are a few examples of disaster recovery:

* + A plan for how the staff should react to a fire outbreak within or near a data center.
  + Instructions on recovering content from a data backup and maintaining normal operations if a web or app server goes down.
  + Guidance on how to resume operations if the company’s cloud ERP system goes down.
  + A strategy for bringing a website back online following a cyber-attack.
  + Instructions on how to protect equipment in a hurricane-prone area and use failover backups to keep services online.
  + Directions on how the team should mitigate the situation if one of the employees accidentally opens a file in a phishing email.
  + A ransomware prevention DR plan that provides steps on how the team should isolate infected systems and use immutable backups to restore data.

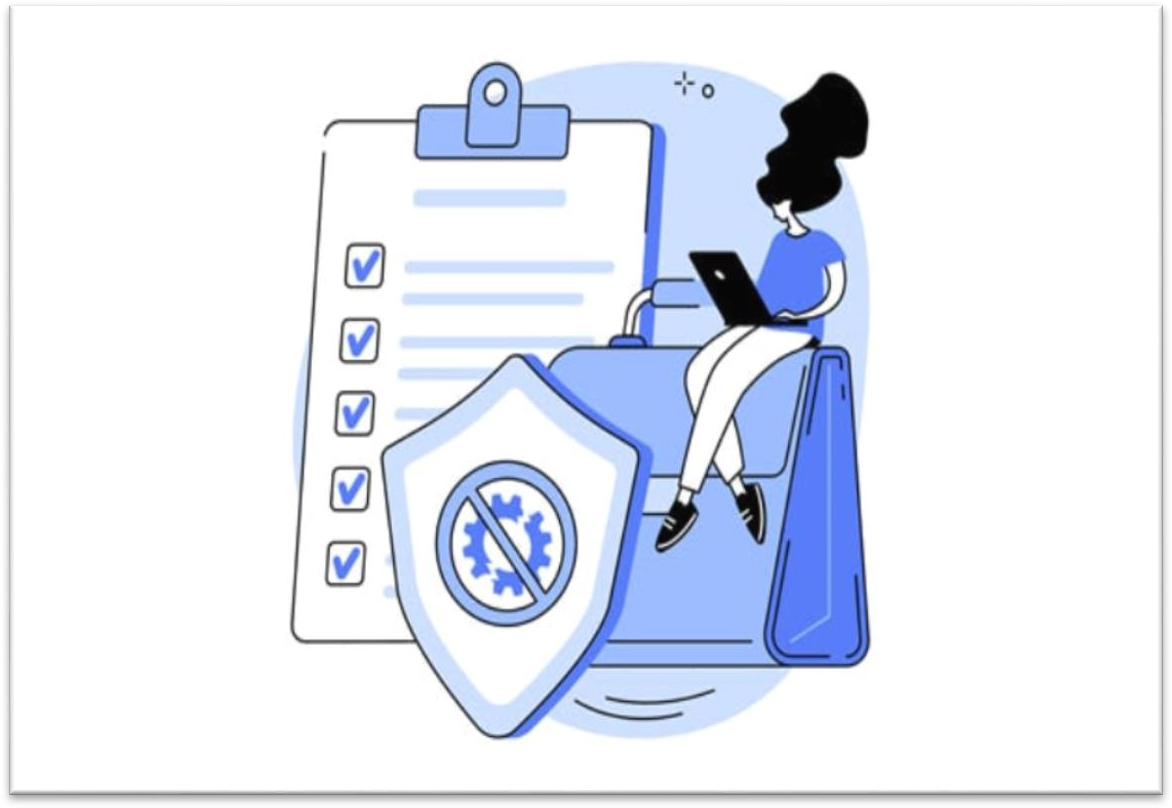
## What Is a Disaster Recovery Plan?

A disaster recovery plan is a company-wide document that specifies how the team should respond to specific disruptions or disasters. This document provides all the information employees need to minimize the effects of the disaster and protect the business.

While every DR plan is unique, each document should include:

* + The disaster plan’s main goals and recovery times.
  + Go-to personnel and their contact info.
  + An overview of potential threats and risks.
  + A breakdown of critical IT assets.
  + A detailed description of response actions and procedures.

A disaster recovery plan should constantly be evolving. Ensure the response strategy remains effective and accurate by updating the document whenever you add new equipment or expand the tool stack.



## Elements of a DR Plan

A well-rounded disaster recovery plan should include the following elements:

* + **Risk analysis:** An evaluation of all the potential risks the business can face.
  + **Business impact analysis:** The BIA assesses the effects of the dangers outlined by the risk analysis. This evaluation predicts potential impacts on a company’s safety, finances, reputation, and compliance.
  + **Disaster recovery goals:** A clear definition of what the organization aims to achieve with the disaster recovery plan.
  + **Recovery Time Object (RTO):** RTO is the time it takes for the IT infrastructure to come back online after an incident. This metric defines the maximum downtime a critical system can experience in case of a disaster.
  + **Recovery Point Object (RPO):** RPO is the acceptable amount of data (measured by time) you can lose between the start of the incident and full IT recovery.
  + **Go-to personnel:** A clear list of names and contacts of staff members responsible for executing the DR plan.
  + **An IT inventory:** A detailed list of hardware and software assets, IT criticality, and dependencies.
  + **Recovery sites:** An overview of all the cold, warm, and hot sites the team can rely on in an emergency.
  + **Backup procedures:** Instructions on how, when, and where you back up resources and how to recover content.
  + **Disaster recovery procedures:** Step-by-step emergency responses for different incident scenarios.
  + **Restoration guides:** Detailed plans for recovering IT operations.

## How to Create a Disaster Recovery Plan?

Below is a step-by-step guide on how to create a basic disaster recovery plan:

* + **Perform risk analysis:** Map out the threats you are most likely to face, including natural disasters, equipment failure, and cyber threats.
  + **Define DR objectives:** Outline the primary goals of the disaster recovery plan and define expected recovery times (RTO and RPO).
  + **Map out assets:** Identify what you are trying to protect, including network equipment, servers, workstations, software, cloud resources, and critical data. List each asset’s location (whether physical or digital), configuration, model, serial number, version, and dependencies.
  + **Prioritize assets:** Define each asset’s priority (high, medium, and low) based on how much the loss would disrupt the business.
  + **Provide an outline of facilities:** Create an in-depth look at your facilities (floor plans, power needs, security requirements, anti-fire mechanisms, etc.).
  + **Define the go-to personnel:** Provide names and contacts of employees and teams responsible for executing DR measures.
  + **Explain backup procedures:** Make a detailed guide on how, when, and where the company backs up data.
  + **Outline disaster recovery procedures:** Provide emergency response procedures for each potential incident.
  + **Explain recovery procedures:** Explain how the team should restore IT operations and data following a disaster. The plan should cover responses to all the threats outlined in the risk analysis.
  + **Write instructions for backup sites:** If the team cannot continue to use the primary data center after the disaster, employees must know how to reach alternative sites (whether cold, warm, or hot).
  + **Provide restoration instructions:** Write a detailed plan for restoring the entire IT setup to a pre-disaster state.

Before you make the plan formal, you should run a realistic drill for each disaster type. You can organize a penetration test for all software-based disasters to see if the procedure works in a real- life setting.



## Forming a Strong DR Team

Whether creating a DR plan from scratch or improving an existing strategy, forming the right team of experts is critical to success. Break your DR team up into four key groups responsible for:

* + **Executive decisions:** These staff members approve DR-related strategies, policies, and budgets.
  + **Crisis management:** This team launches recovery plans, coordinates restoration efforts, and handles unforeseen problems. These employees are the go-to contact for all DR-related issues.
  + **Operational continuity:** These experts are responsible for business continuity best practices and ensuring services stay available during the disaster.
  + **Impact assessment and recovery:** This team assesses the damage and leads the recovery phase of the DR plan.

Training is the key to creating a capable DR team. Run regular drills and tests to keep employees in good form and ensure the DR team stays up to date with the changes to the IT environment.

***Hope for the Best, Plan for the Worst***

The longer you take to recover from an incident, the greater the impact on your operations and finances. A sound DR plan ensures rapid recovery from disruptions and, as such, must be an integral part of your IT and business strategy.