**DISASTER RCOVERY**

1. **What is meant by 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.



1. **What is the purpose of disaster recovery?**

The purpose of a disaster recovery plan is to comprehensively explain the consistent actions that must be taken before, during, and after a natural or man-made disaster so that the entire team can take those actions.

### What is a disaster?

The practice of DR revolves around events that are serious in nature. These events are often thought of in terms of natural disasters, but they can also be caused by systems or technical failure or by humans carrying out an intentional attack. They are significant enough to disrupt or completely stop critical business operations for a period of time.

1. **Types of Disasters**

There are three categories of disasters we’ll cover in this blog:

1. Natural Disasters
2. Physical Disasters
3. Technology-Based Disasters

### Benefits of a disaster recovery plan

### 

### Types of disaster recovery

In addition to choosing a DR site and considering DR tiers, IT and business leaders must evaluate the best way to put their DR plan into action. This will depend on the IT environment and the technology the business chooses to support its DR strategy.

* Network disaster recovery
* Data center disaster recovery
* Virtualized disaster recovery
* Cloud disaster recovery
* Disaster recovery as a service (DRaaS)

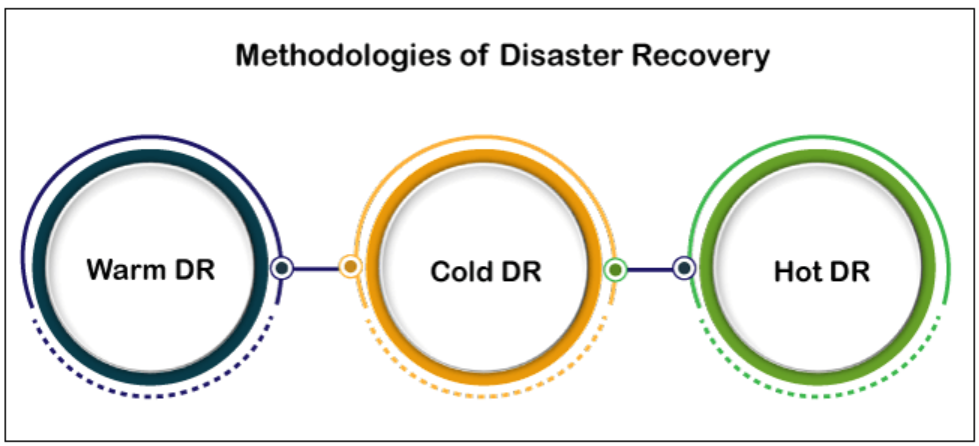
## **What is a disaster recovery plan?**

Organizations of all sizes generate and manage massive amounts of data, much of it mission critical. The impact of corruption or data loss from human error, hardware failure, malware, or hacking can be substantial. Therefore, it is essential to create a disaster recovery plan for the restoration of business data from a data backup image.

It is most effective to develop an information technology (IT) disaster recovery plan in conjunction with the business continuity plan (BCP). A business continuity plan is a complete organizational plan that consists of five components:

1. Business resumption plan  
2. Occupant emergency plan  
3. Continuity of operations plan  
4. Incident management plan (IMP)  
5. Disaster recovery plan

1. **Methodologies of Disaster recovery**



* **Warm disaster recovery**---- An equipped data center that doesn't have customer data; an organization can install additional equipment and introduce customer data following a disaster.
* **Cold disaster recovery**---- Has infrastructure to support IT systems and data, but no technology until an organization activates DR plans and installs equipment; they are sometimes used to supplement hot and warm sites during a long-term disaster.
* **Hot disaster recovery**--- A fully functional data center with hardware and software, personnel, and customer data, which is typically staffed around the clock and operationally ready in the event of a disaster.

## **What should a disaster recovery plan include?**

* **Goals--** A statement of goals will outline what the organization wants to achieve during or after a disaster, including the recovery time objective (RTO) and the recovery point objective (RPO).
* **Personnel----** Every disaster recovery plan must detail the personnel who are responsible for the execution of the DR plan and make provisions for individual people becoming unavailable.
* **IT inventory---** An updated IT inventory must list the details about all hardware and software assets, as well as any cloud services necessary for the company’s operation, including whether they are business critical, and whether they are owned, leased, or used as a service.
* **Backup procedures---** The DRP must set forth how each data resource is backed up – exactly where, on which devices and in which folders, and how the team should recover each resource from backup.
* **Disaster recovery procedures** --- These specific procedures, distinct from backup procedures, should detail all emergency responses, including last-minute backups, mitigation procedures, limitation of damages, and eradication of cybersecurity threats.
* **Disaster recovery sites---** Any robust disaster recovery plan should designate a hot disaster recovery site. Located remotely, all data can be frequently backed up to or replicated at a hot disaster recovery site — an alternative data center holding all critical systems. This way, when disaster strikes, operations can be instantly switched over to the hot site.
* **Restoration procedures---** Finally, follow best practices to ensure a disaster recovery plan includes detailed restoration procedures for recovering from a loss of full systems operations. In other words, every detail to get each aspect of the business back online should be in the plan, even if you start with a disaster recovery plan template. Here are some procedures to consider at each step.

### Elements of a disaster recovery strategy

Before an organization can determine its DR strategies, it must first analyze existing assets and priorities. Two different analyses typically factor into DR decision-making:

#### **Risk analysis**----- Risk analysis or risk assessment is an evaluation of all the potential risks the business could face, as well as their outcomes. Risks can vary greatly depending on the industry the organization is in and its geographic location. The assessment should identify potential hazards, determine who or what these hazards would harm, and use the findings to create procedures that take these risks into account.

#### **Business impact analysis**--- Business impact analysis (BIA) evaluates the effects of the risks identified above to business operations. A BIA can help predict and quantify costs, both financial and non-financial. It also examines the impact of different disasters on an organization's safety, finances, marketing, business reputation, legal compliance and quality assurance.

#### **Recovery point objective**--- [RPO](https://www.techtarget.com/whatis/definition/recovery-point-objective-RPO) is the maximum age of files that an organization must recover from backup storage for normal operations to resume after a disaster. The RPO determines the minimum frequency of backups. For example, if an organization has an RPO of four hours, the system must back up at least every four hours.

#### **Recovery time objective**---- [RTO](https://www.techtarget.com/whatis/definition/recovery-time-objective-RTO) refers to the amount of time an organization estimates its systems can be down without causing significant or irreparable damage to the business. In some cases, applications can be down for several days without severe consequences. In others, seconds can do substantial harm to the business.

## **Steps involved in creating a disaster recovery plan**

There are several guidelines that one can follow to create a DRP, such as a list of hardware and software ranked in order of priority, a list stating who is responsible for what, and the identification of backup employees. Additionally, one should always test their DRP regularly to ensure that it is as best as it could be. Furthermore, there are several steps required to create a successful DRP.

### 1.Create an inventory list

Every company should know exactly which IT resources—systems, hardware, and software—are used to run the business. In addition to a simple [inventory management system](https://blog.trginternational.com/infor-eam-keeps-the-worlds-largest-machine-running), it can be helpful to add different scenarios to your IT disaster recovery plan. Ask yourself, which systems would be affected in the event of a flood, hurricane, fire, or power outage on your premises?

### 2. Establish a recovery timeline

Once you’ve documented your IT inventory, you can decide on the acceptable recovery goals and timeframes by which certain systems need to be back in operation. Industries such as healthcare may have a recovery timeline of mere minutes, while other industries may find longer timelines to be tolerable.

### 3. Communication

Before a disaster strikes, get information from key stakeholders. Everyone should understand which IT operations are potentially affected, what would happen next, and who would be responsible for resolving the issues. Ask employees how their work would be impacted if certain systems or networks were unavailable for a while. You should also create a plan for communicating with your staff in the event of a power or Internet outage.

### 4. Back up your data

Your options for data backups include [cloud storage](https://blog.trginternational.com/cloud-services-fundamentals), internal off-site data backups, and vendor-supported backups. Maintaining your backups physically on-premises is not acceptable due to the risk of a natural disaster. Both physical and cloud backups have their risks. Working with a [trusted managed services partner](https://blog.trginternational.com/what-hoteliers-need-to-know-about-managed-it-services) can help you weigh the issue and decide which is the better option for your circumstances.

* Using the 3-2-1 backup rule (keep 3 copies of your data, keep 2 copies on different backup mediums, keep 1 copy offsite)
* Ensuring that backups are regularly monitored
* Testing data restoration regularly
* Backing up all devices (including smartphones and tablets)
* Backing up cloud services (Microsoft 365, etc.)

Data backup and recovery should be an integral part of the business continuity plan and information technology disaster recovery plan. Developing a **data backup strategy** begins with identifying what data to backup, selecting and implementing hardware and software backup procedures, scheduling and conducting backups, and periodically validating data to ensure it has been properly stored**3**.

### 5. Consider insurance

Purchasing catastrophe insurance as part of a disaster recovery plan can be an interesting option if you’re worried about the costs of recovery. This means not just replacing your IT equipment but examining the broader consequences and losses following a disaster. If this idea appeals to you, please consult with an insurance professional.

### 6. Test your disaster recovery plan

Your IT disaster recovery plan should be tested at least once, and preferably twice, per year. After not testing their plan for several years, one of our clients discovered that all of their drives failed to restore. If this had occurred during a real disaster, the data would have been lost forever. Any gaps that you identify during these tests should be documented extensively for further investigations and mitigations. Work with a trusted managed service provider to learn about your options for remediation.

### Run Disaster Recovery Drills

Disaster recovery plans might look great on paper but fail when they are needed most. To avoid this from happening, run a drill and test your plan in a realistic scenario. Learn the lessons from the drill and update the plan to make it clearer and more effective for all parties involved. Disaster recovery plans must be updated at least once per year.