

DISASTER RECOVERY

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **S.No.** | **Title** | **Page No.** |
| 1 | What is Disaster Recovery? | 1 |
| 2 | Why is disaster recovery important? | 2-3 |
| 3 | How does disaster recovery work? | 4-5 |
| 4 | What are the key elements of a disaster recovery plan? | 6-7 |
| 5 | How can you create a disaster recovery team? | 8 |
| 6 | What are the best disaster recovery methods? | 9-11 |
| 7 | How can AWS help with disaster recovery? | 11 |

# What is Disaster Recovery?

* + Disaster recovery is the process by which an organization anticipates and addresses technology-related disasters.
  + IT systems in any company can go down unexpectedly due to unforeseen circumstances, such as power outages, natural events, or security issues.
  + Disaster recovery includes a company's procedures and policies to recover quickly from such events.

# Why is disaster recovery important?

* + An IT system. Outages come in many forms, including the following examples.
    - An earthquake or fire.
    - Technology failures.
    - System incompatibilities.
    - Simple human error.
    - Intentional unauthorized access by third parties.
  + These disasters disrupt business operations, cause customer service problems, and result in revenue loss.
  + A disaster recovery plan helps organizations respond promptly to disruptive events and provides key benefits.

## Ensures business continuity

* + When a disaster strikes, it can be detrimental to all aspects of the business and is often costly.
  + It also interrupts normal business operations, as the team’s productivity is reduced due to limited access to tools they require to work.
  + A disaster recovery plan prompts the quick restart of backup systems and data so that operations can continue as scheduled.

## Enhances system security

* + Integrating data protection, backup, and restoring processes into a disaster recovery plan limits the impact of ransomware, malware, or other security risks for business.
  + For example, data backups to the cloud have numerous built-in security features to limit suspicious activity before it impacts the business.

## Improves customer retention

* + If a disaster occurs, customers question the reliability of an organization’s security practices and services.
  + The longer a disaster impacts a business, the greater the customer frustration.
  + A good disaster recovery plan mitigates this risk by training employees to handle customer inquiries.
  + Customers gain confidence when they observe that the business is well-prepared to handle any disaster.

## Reduces recovery costs

* + Depending on its severity, a disaster causes both loss of income and productivity.
  + A robust disaster recovery plan avoids unnecessary losses as systems return to normal soon after the incident.
  + For example, cloud storage solutions are a cost-effective data backup method. You can manage, monitor, and maintain data while the business operates as usual.

# How does disaster recovery work?

Disaster recovery focuses on getting applications up and running within minutes of an outage. Organizations address the following three components.

## Prevention

* + To reduce the likelihood of a technology-related disaster, businesses need a plan to ensure that all key systems are as reliable and secure as possible.
  + Because humans cannot control a natural disaster, prevention only applies to network problems, security risks, and human errors.
  + You must set up the right tools and techniques to prevent disaster.
  + For example, system-testing software that auto-checks all new configuration files before applying them can prevent configuration mistakes and failures.

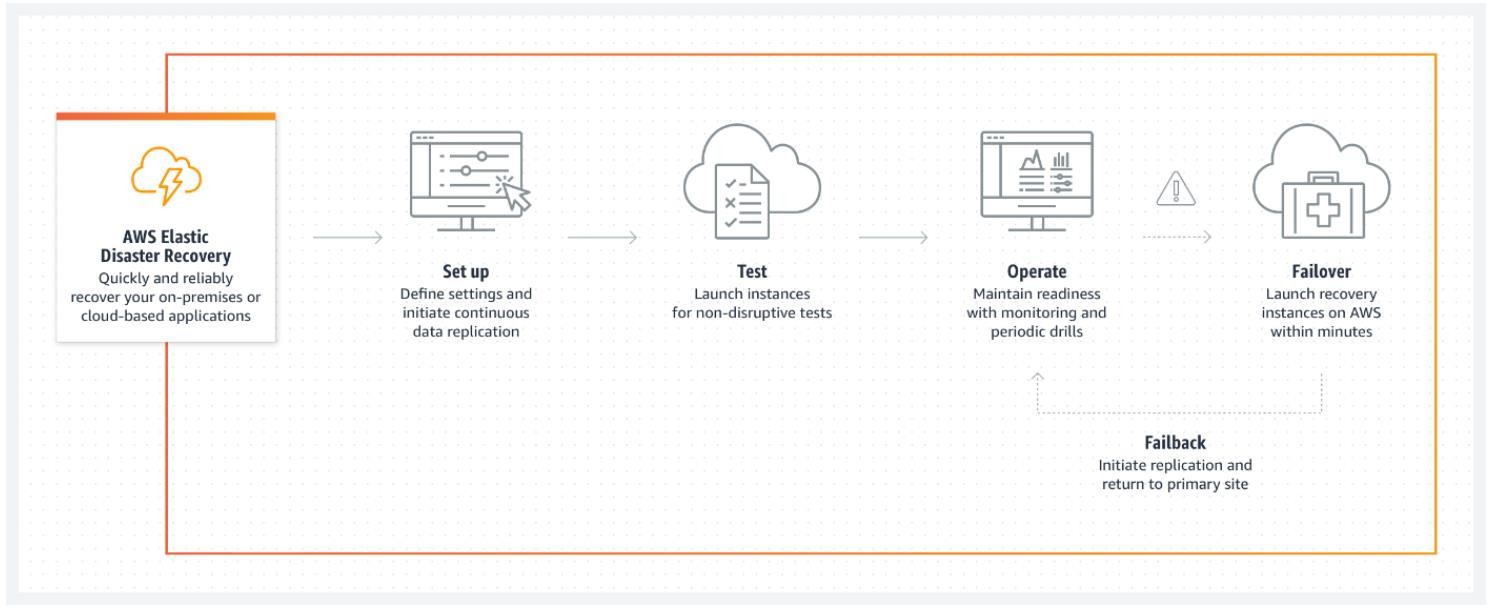
## Anticipation

* + Anticipation includes predicting possible future disasters, knowing the consequences, and planning appropriate disaster recovery procedures.
  + It is challenging to predict what can happen, but you can come up with a disaster recovery solution with knowledge from previous situations and analysis.
  + For example, backing up all critical business data to the cloud in anticipation of future hardware failure of on-premises devices is a pragmatic approach to data management.

## Mitigation

Mitigation is how a business responds after a disaster scenario. A mitigation strategy aims to reduce the negative impact on normal business procedures. All key stakeholders know what to do in the event of a disaster, including the following steps.

* + - Updating documentation.
    - Conducting regular disaster recovery testing.
    - Identifying manual operating procedures in the event of an outage.
    - Coordinating a disaster recovery strategy with corresponding personnel.



# What are the key elements of a disaster recovery plan?

An effective disaster recovery plan includes the following key elements.

## Internal and external communication

* + The team responsible for creating, implementing, and managing the disaster recovery plan must communicate with each other about their roles and responsibilities.
  + If a disaster happens, the team should know who is responsible for what and how to communicate with employees, customers, and each other.

## Recovery timeline

* + The disaster recovery team must decide on goals and time frames for when systems should be back to normal operations after a disaster.
  + Some industries’ timelines may be longer than others, while others need to be back to normal in a matter of minutes.
  + The timeline should address the following two objectives.

### Recovery time objective.

* + - * The recovery time objective (RTO) is a metric that determines the maximum amount of time that passes before you complete disaster recovery.
      * Your RTOs may vary depending on impacted IT infrastructure and systems.

### Recovery point objective.

* + - * A recovery point objective (RPO) is the maximum amount of time acceptable for data loss after a disaster.
      * For example, if your RPO is minutes or hours, you will have to back up your data constantly to mirror sites instead of just once at the end of the day.

## Data backups.

* + The disaster recovery plan determines how you back up your data. Options include
    - Cloud storage.
    - Vendor-supported backups, and
    - Internal offsite data backups.
  + To account for natural disaster events, backups should not be onsite. The team should determine who will back up the data, what information will be backed up, and how to implement the system.

## Testing and optimization.

* + You must test your disaster recovery plan at least once or twice per year. You can document and fix any gaps that you identify in these tests.
  + Similarly, you should update all security and data protection strategies frequently to prevent inadvertent unauthorized access.

# How can you create a disaster recovery team?

A disaster recovery team includes a collaborative team of experts, such as IT specialists and individuals in leadership roles, who will be crucial to the team. You should have somebody on the team who takes care of the following key areas.

## Crisis management

* + The individual in charge of crisis management implements the disaster recovery plan right away.
  + They communicate with other team members and customers, and they coordinate the disaster recovery process.

## Business continuity

* + The business continuity manager ensures that the disaster recovery plan aligns with results from business impact analysis.
  + They include business continuity planning in the disaster recovery strategy.

## Impact recovery and assessment

* + Impact assessment managers are experts in IT infrastructure and business applications.
  + They assess and fix network infrastructure, servers, and databases.
  + They also manage other disaster recovery tasks, such as the following examples.
    - Application integrations.
    - Data consistency maintenance.
    - Application settings and configuration.

# What are the best disaster recovery methods?

When disaster recovery planning, businesses implement one or several of the following methods.

## Backup

* + Backing up data is one of the easiest methods of disaster recovery that all businesses implement.
  + Backing up important data entails storing data offsite, in the cloud, or on a removable drive.
  + You should back up data frequently to keep it up to date.
  + For example, by backing up to AWS, businesses get a flexible and scalable infrastructure that protects all data types.

## Data center disaster recovery

* + In the event of certain types of natural disasters, appropriate equipment can protect your data center and contribute to rapid disaster recovery.
  + For example, fire suppression tools help equipment and data survive through a blaze, and backup power sources support businesses’ continuity in case of power failure.
  + Similarly, AWS data centers have innovative systems that protect them from human-made and natural risks.

## Virtualization

* + Businesses back up their data and operations using offsite virtual machines (VMs) not affected by physical disasters.
  + With virtualization as part of the disaster recovery plan, businesses automate some processes, recovering faster from a natural disaster.
  + The continuous transfer of data and workloads to VMs like Amazon Elastic Compute Cloud (Amazon EC2) is essential for effective virtualization.

## Disaster recovery as a service

* + Disaster recovery services like AWS Elastic Disaster Recovery can move a company’s computer processing and critical business operations to its own cloud services in the event of a disaster.
  + Therefore, normal operations can continue from the provider’s location, even if on-premises servers are down.
  + Elastic Disaster Recovery also protects from regions in the cloud going down.

## Cold site

* + In the event of a natural disaster, a company moves its operations to another rarely used physical location, called a cold site.
  + This way, employees have a place to work, and business functions can continue as normal.
  + This type of disaster recovery does not protect or recover important data, so another disaster recovery method must be used alongside this one.

# How can AWS help with disaster recovery?

Elastic Disaster Recovery is a disaster recovery service that reduces downtime and data loss with the fast, reliable recovery of on-premises and cloud-based applications. It can decrease your RPO to seconds and RTO to just a few minutes. You can quickly recover operations after unexpected events, such as software issues or data center hardware failures. It is also a flexible solution, so you can add or remove replicating servers and test various applications without specialized skill sets.

* + Elastic Disaster Recovery includes the following benefits.
    - Reduces costs by removing idle recovery site resources, so you pay for the full disaster recovery site only when needed.
    - Converts cloud-based applications to run natively on AWS.
    - Restores applications within minutes, at their most up-to-date state, or from a previous point in time in case of security incidents.