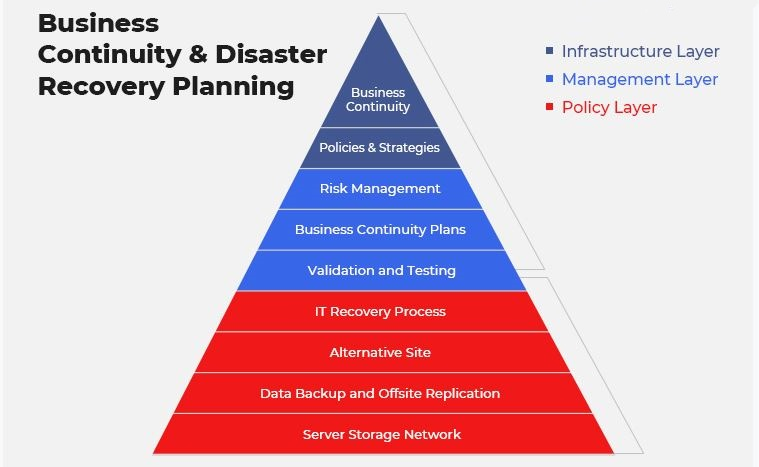
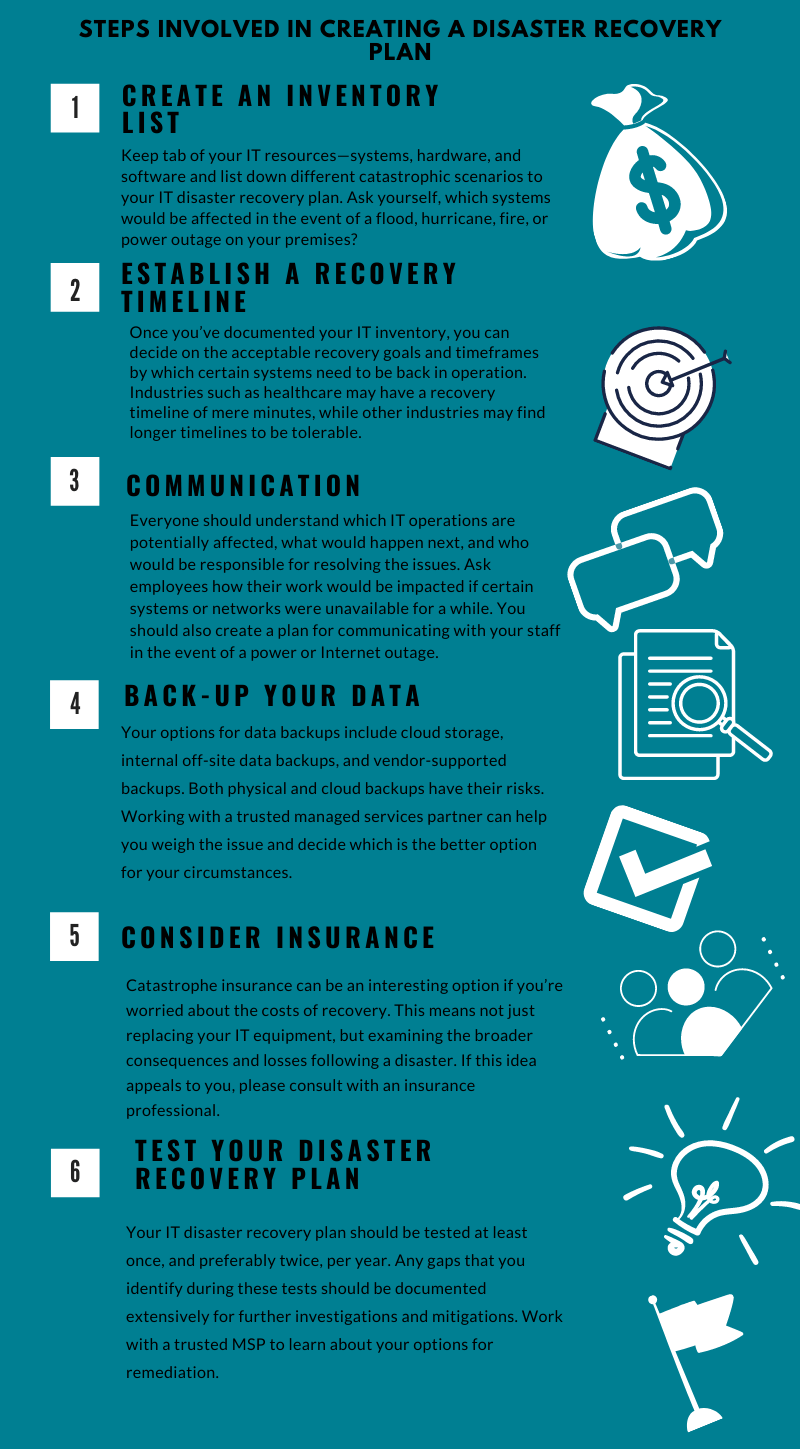
**DISASTER RECOVERY** **What exactly is a disaster recovery plan?**Disaster recovery is an organization’s method of regaining access and functionality to its IT infrastructure after events like natural disasters, power outages, cyber-attacks, or even business disruptions related to the COVID-19 pandemic.  
Depending on the business affected, a variety of solutions can be part of a disaster recovery plan. As DR is one aspect of business continuity, planning for disasters, whether natural or man-made, should be just as high a priority for businesses as having a proactive growth plan. **Why is disaster recovery plan necessary?**Disaster recovery operations are different for every industry, but with the advent of remote and hybrid working and the rapid evolution of technology, organizations worldwide need a basic set of protocols for the following reasons:

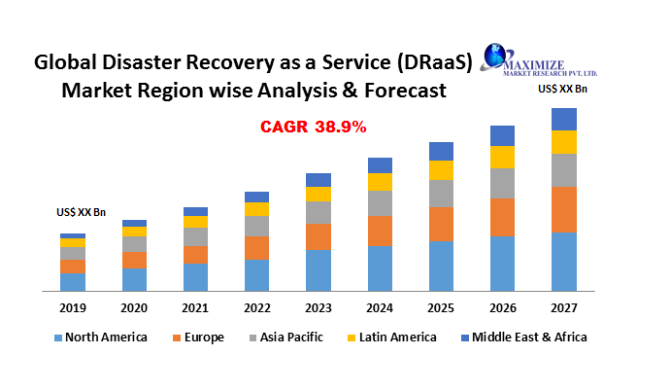
* The dependency on computer networks and electronic delivery systems increases the odds of everyday businesses being disrupted by failure of one of their core systems.
* A formal process to deal with potential accidents, disasters, data breaches or outages is needed and, in some industries, required.
* Everyone wants to lower the potential costs of dealing with a disaster.
* Because of the speed at which technology is changing, there is an increased chance that knowledge gaps can lead to inadequate IT security precautions.
* An effective system to backup and recovery essential business data is vital in case of network shutdown.
* Avoiding the potential failure of a business and the collapse of its IT infrastructure in the face of an unforeseen, catastrophic event.

**How does disaster recovery work?**Disaster recovery relies on replicating data and computer processing in an off-premises location not affected by the disaster. When physical servers go down and data loss is threatened because of a natural disaster, equipment failure or cyber-attack, a business needs to recover lost data from an alternative location where the data is backed up.  
Ideally, an organization can transfer its computer processing to that remote location as well in order to ensure data protection and continue operations.

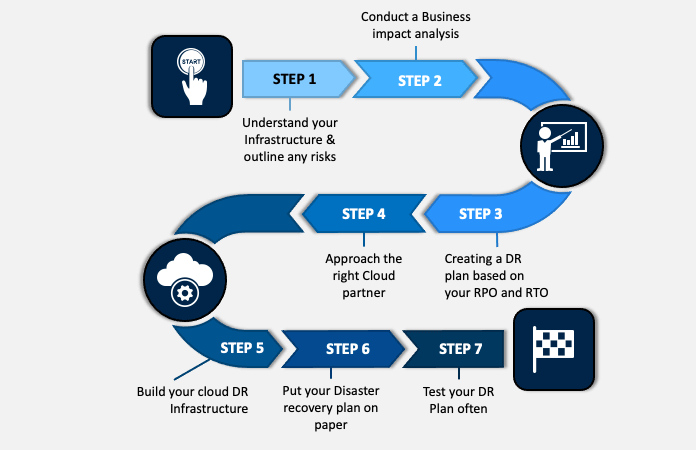
**Steps to creating a disaster recovery plan**Organizations can follow certain pre-determined guidelines when creating a DR plan, like listing an inventory of hardware and software ranked in order of priority. A list stating who is responsible for what, and the identification of backup employees. Additionally, businesses should review and [test their DR plan](https://www.ir.com/guides/disaster-recovery-testing) regularly to ensure that it works.

****

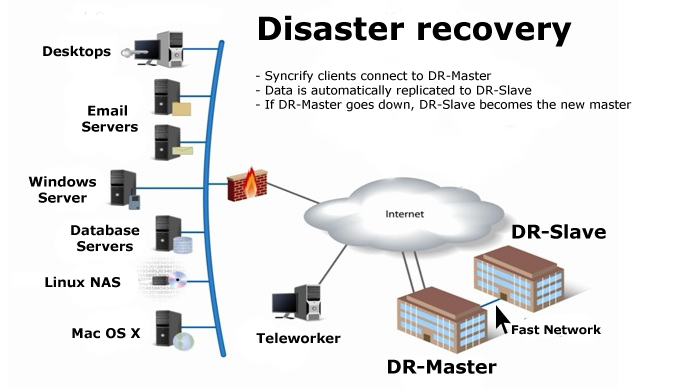
## What are the different types of disaster recovery? Organizations can implement a variety of disaster recovery methods, or combine several, depending on the nature of the disaster, the type of organization, its infrastructure, and its own disaster recovery plan: Back-upBackup solutions are the simplest type of DR and entail storing data at an offsite data center, 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 SiteIn these types of DR solutions, an organization sets up a basic infrastructure in an alternative facility that provides a place for employees to work after a natural disaster or fire. It can help with business continuity, allowing a company's operations to continue, but does not provide data management, data protection, or recovery. Cold site solutions should be combined with other methods of disaster recovery. Hot SiteHot site solutions facilitate data management by always maintaining up-to-date copies of data. Hot sites are time-consuming to set up and more expensive than cold sites, but they can dramatically reduce down time, which can save costs in the long run. Back Up as a Service (BaaS)Backup as a service (BaaS) is a solution for data management that involves purchasing backup and recovery services from an online data backup provider. Instead of performing backup with a centralized, on-premises IT department, Backup as a Service solutions connect systems to a private, public or hybrid cloud managed by the outside provider. Datacenter disaster recoveryThe physical elements of a data center can protect data and contribute to faster disaster recovery and efficient data management 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 DR solutions will help in the event of a cyber-attack. VirtualizationOrganizations can back up certain operations and data or even a working replica of their entire computing environment on off-site virtual servers and virtual machines that are unaffected by physical disasters. Using virtualization as part of disaster recovery solutions 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 copiesPoint-in-time copies, or 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 virtual machines that are unaffected by the disaster. Instant recoveryInstant recovery is similar to point-in-time copies, except that instead of copying data from your database, instant recovery takes a snapshot of an entire virtual machine.   Disaster Recovery as a Service (DRaaS) With the rapid increase of cloud services, comes a variety of IT solutions that are available as a service instead of being purchased. One of the most important ones is Disaster Recovery as a Service or DRaaS.



DRaaS solutions are important for data protection, data backup and management in the event of a disaster. They are an innovative and less costly way to back up critical data and quickly recover critical systems after a disaster. Disaster recovery services do this by leveraging cloud‐based resources that provide less expensive infrastructure than on-premises systems due to the ability to scale and share cloud resources.



To meet the growing demand for software resilience, DraaS providers have brought simplification and reduced costs to organization.  
With Disaster Recovery as a Service, an organization can implement a high‐performing disaster recovery solution for its critical systems and reduce the complexity of the disaster recovery process. Like other as-a-service providers, DRaaS providers take care of the back‐end complexity for their customers and provide a simple user interface for setting up and managing a disaster recovery solution.



## DRaaS benefits A DRaaS solution represents the next generation of rapid system data recovery and always‐on availability, helping organizations avoid downtime and business disruption without the excessive costs associated with traditional hot sites. The low cost and simplicity of Disaster Recovery as a Service makes it available to an entirely new class of organizations. The ability to recover applications in the cloud, if needed, slashes the cost and complexity of recovery capabilities. Organizations previously unsure about implementing DR solutions can now enjoy capabilities that were once reserved for large enterprises.

## DRaaS and virtualization Virtualization is the technology that permits multiple operating system instances to run on each physical server. The power of virtualization has contributed significantly to the power of Disaster Recovery as a Service. Some DRaaS solutions can provide advanced, imaged‐based virtual machine (VM) replication, which can be used to send VM images to a cloud service provider. Service providers can provide virtual cloud hosts; recovering your server is as easy as booting those hosts from the images sent from your primary site. Best disaster recovery solutions include agentless components, meaning there is no software present within individual virtual machines. Instead, a module is installed in the virtual environment, which intercepts local disk traffic and sends it to your cloud service provider, where another module receives the traffic and keeps your server VM’s and databases up to date, usually within minutes.

## Which DRaaS service is best? ****Managed DRaaS**** In a fully managed Disaster Recovery as a Service model, a third party takes over all responsibility for disaster recovery, including critical applications. Choosing this option requires an organization to stay in close contact with their DRaaS provider to ensure that it stays up to date on all infrastructure, application, and services changes. If you lack the expertise or time to manage your own disaster recovery, a fully managed option may be the best. ****Assisted DRaaS**** If you prefer to maintain responsibility for some aspects of your disaster recovery solution, or if you have unique or customized applications that might be challenging for a third party to take over, assisted DRaaS might be a better option. In this model, the service provider offers its expertise for optimizing disaster recovery procedures, but the customer is responsible for implementing some or all of the DR plan. ****Self-service DRaaS**** The least expensive option is self-service DRaaS, where the customer is responsible for the planning, testing and management of disaster recovery, and the customer hosts its own infrastructure backup on virtual machines in a remote location. Careful planning and testing are required to make sure that processing can fail over to the virtual servers instantly in the event of a disaster. This option is best for those who have experienced disaster recovery experts on staff.

## A monitoring and performance management solution should be part of every DR plan Having third party monitoring tools in place is part of every organization's best disaster recovery solution. Monitoring solutions can help to avoid certain disasters or at least reduce their severity by picking up anomalies within a system and identifying potential issues.  [IR Collaborate](https://www.ir.com/products/collaborate) provides the insights an organization needs to make initiative-taking business decisions, formulate effective DR plans, and create an efficient production environment.

* Comprehensive monitoring, surveillance, alerting, and reporting helps you meet and manage your SLAs by ensuring your systems and applications are running at peak performance.
* Gather real time intelligence across a wide range of data points and criteria
* Customizable dashboards provide deep visibility that can help identify problems in real time. This allows you to take immediate action to solve issues before they impact the broader business.

**Conclusion :** Disasters are negative disruptive events bound to occur and organizations need to develop strategies to withstand its effects. IT organizations require a strategy or recovery plan that can help them rebound in the face of disasters. Disaster recovery plans (DRPs) are effective in helping bridge and manage disasters.   
They should be developed around the organization’s business continuity needs and should be reviewed frequently since business continuity needs evolve over time.