

What is disaster rec



Security



What is DR?

Disaster recovery (DR) consists of I designed to prevent or minimize da resulting from catastrophic events-

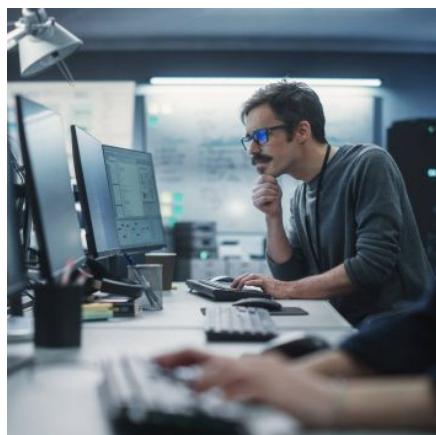
failures and localized power outage emergencies, criminal or military attacks. Many businesses—especially small- and medium-sized enterprises—need a reliable, practicable disaster recovery plan. This plan provides protection from the impact of significantly different types of disasters.

Infrastructure failure can cost as much as [US\\$100 million](#). Application failure costs can range from US\$100,000 to US\$10 million. Businesses cannot recover from such losses. Some businesses do not re-open after experiencing a disaster, another 20% will fail within the first year after the crisis. Implementing a disaster recovery plan can reduce these risks.

Disaster recovery planning involves strategic planning, technology, and continuous testing. Maintaining a disaster recovery plan is a key component of disaster recovery planning, but it does not constitute a full disaster recovery plan.

Disaster recovery also involves ensuring that resources are available to maintain robust failover and fail-safe mechanisms. This includes offloading workloads to backup systems so that business operations are disrupted as little as possible during a disaster, and recovering from original primary systems.

Read our article to learn more information about [disaster recovery planning](#).



Strengths

Stay ahead of security, AI, and

Subscribe

Business continuity

Business continuity planning creates system your enterprise will be able to maintain essential operations as quickly as possible in the event of a crisis. Disaster recovery planning is the subset of business continuity planning that focuses on protecting infrastructure and systems.

Disaster recovery planning

Business impact analysis

The creation of a comprehensive disaster recovery plan begins with a business impact analysis. When performing this analysis, you identify critical business processes and scenarios that can then be used to predict the potential impact of a disaster if certain business processes were disrupted. What would happen if a server was destroyed by fire, for instance? Or an employee was unable to access critical data?

This will allow you to identify the areas and resources that are most critical and enable you to determine how much time each function could tolerate. With this information, you can create a plan for how the most critical operations could be restored quickly.

IT disaster recovery planning should follow the same basic steps as business impact analysis. If, for instance, your business continues to operate during a disaster, you may need to have IT representatives to work from home in the affected area. What hardware, software, and IT resources would be required to support this?

Risk analysis

Assessing the likelihood and potential consequences of various risks is also an essential component of disaster recovery planning. As ransomware become more prevalent, it's crucial to understand the cybersecurity risks that all enterprises face. This includes risks specific to your industry and geographical location.

For a variety of scenarios, including natural disasters, cyber attacks, and人为错误, you can estimate the overall impact on your business. Ask yourself:

- What financial losses due to missed sales or generating activities would you incur?

- What kinds of damage would your brand customer satisfaction be impacted?
- How would employee productivity be impacted?
- What risks might the incident pose to humans?
- Would progress towards any business initiatives be lost?

Prioritizing applications

Not all workloads are equally critical to your business. Downtime is far more tolerable for some systems than others. Prioritize your systems and applications into three tiers based on how important it is for them to be up and how serious the impact would be if they were down.

1. **Mission-critical:** Applications whose failure would have a significant impact on your business survival.
2. **Important:** Applications for which you can tolerate some downtime.
3. **Non-essential:** Applications you could temporarily live without or do without.

Documenting dependencies

The next step in disaster recovery planning is to document all hardware and software assets. It's essential to understand the interdependencies at this stage. If one software component goes down, what other components will be affected?

Designing resiliency—and disaster recovery—into your architecture is the best way to manage application dependencies in today's **microservices**-based architectures. It's important to know what happens when other systems or processes are down, what kind of situation to recover from, and it's vital to understand how to develop alternate plans for your systems in case of strikes.



Establishing recovery time objectives, recovery point objectives, and recovery consistency objectives

By considering your risk and business impact, you can determine your recovery time objectives for how long you'd need it to take to get your business up and running again. You could stand to use, and how much data you could afford to lose.

Your recovery time objective (RTO) is the maximum amount of time you have to restore application or system functioning following a disaster.

Your recovery point objective (RPO) is the maximum age of data that must be recovered in order for your business to resume operations. Businesses, losing even a few minutes' worth of data, may not be able to tolerate losing data. In other industries, such as financial services, losing even a few minutes' worth of data may be able to tolerate losing data.

A recovery consistency objective (RCO) is established through a service level agreement (SLA) for continuous data protection services. It specifies how often inconsistent entries in business data from recovery points are tolerable in disaster recovery situations, depending on the complexity of the application environments.

Regulatory compliance

All disaster recovery software and solutions must satisfy any data protection and security regulations that your business adheres to. This means that all data backup and recovery processes must meet the same standards for ensuring data integrity and availability as primary systems.



At the same time, several regulatory standards require businesses to maintain disaster recovery and/or business continuity plans. Sarbanes-Oxley (SOX), for instance, requires all publicly held companies to maintain accurate business records for a minimum of five years. Failing to do so can result in significant financial penalties for companies.

Choosing technologies

Backups serve as the foundation upon which In the past, most enterprises relied on tape maintaining multiple copies of their data and

In today's always-on digitally transforming world, we often cannot achieve the RTOs necessary to meet business needs. Architecting your own disaster recovery solution requires a deep understanding of the capabilities of your production environment and the resources available. Support staff, administration, facilities, and organizations are turning to cloud-based backup and recovery services provided by Recovery-as-a-Service (DRaaS) providers.

Choosing recovery site location

Building your own disaster recovery plan requires careful consideration of your data center objectives. On the one hand, a copy of your data should be geographically distant enough from your headquarters to be affected by the same seismic events, ensuring it remains operational if your main site is damaged. On the other hand, backups should be located closer than those located on-premises at the primary site, or even greater across longer distances.

Continuous testing and maintenance

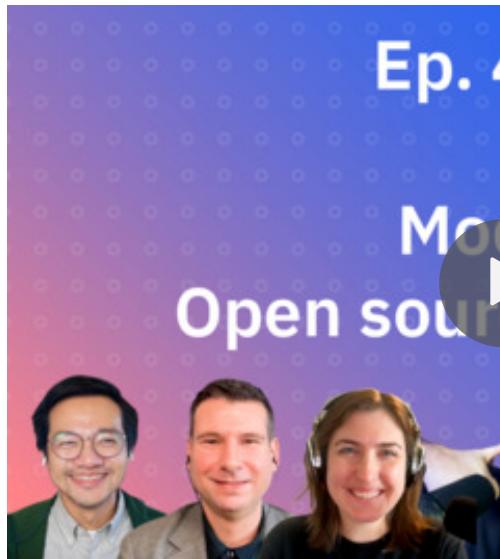
Simply put, if your disaster recovery plan has been tested and maintained, it will work. All employees with relevant responsibilities should participate in a test exercise, which may include maintaining the plan for a specific period of time.

If performing comprehensive disaster recovery tests is not feasible due to resource constraints or capabilities, you can also schedule a "tabletop" exercise. While this type of exercise does not involve actual procedures, though you should be aware that it can help identify potential anomalies or weaknesses in your DR plan. By identifying these issues before they occur, you can prevent previously undiscovered application interdependencies from causing significant downtime.

As your hardware and software assets change over time, your disaster recovery plan gets updated as needed. It's important to revise the plan on an ongoing basis.

The IBM Knowledge Center provides an extensive library of resources for disaster recovery planning.

Mixture of Experts | 31 January, episode 1



Decoding AI: Weekly News |

Join our world-class panel of engineers, leaders and more as they cut through the latest in AI news and insights.

[Watch the latest podcast episodes →](#)

Disaster Recovery-as-a-Service (DRaaS)

Disaster-Recovery-as-a-Service (DRaaS) is one of the managed IT service offerings available today. DRaaS providers offer RPOs in a service-level agreement (SLA) that align with your application recovery expectations.

DRaaS vendors typically provide cloud-based disaster recovery services, which can result in significant cost savings compared with maintaining resources in your own data center. Contracting with a DRaaS vendor provides failover capabilities plus the peace of mind of knowing that your data will be recovered in the event of a disaster. Your vendor will be responsible for configuring and maintaining the failover environment.

Disaster recovery service offerings differ from their offering as a comprehensive, all-in-one

services ranging from single application recovery to full cloud. Some offerings may include disaster recovery, while others will charge an additional consulting fee.

Be sure that any enterprise software application you're using with public cloud providers that you're working with has good application performance is satisfactory in the event of a failure. Failover and fallback procedures have been

Cloud DR

If you have already built an on-premises disaster recovery solution, it's challenging to evaluate the costs and benefits of switching to a monthly DRaaS subscription instead.

Most on-premises DR solutions will incur considerable costs for maintenance and administration, software, and upfront capital expenditures involved in the solution. You'll need to budget for regular software upgrades. Because your DR solution must remain compatible with your primary production environment, you'll want to ensure that your DR solution has the same software versions. Depending upon the specifics of your licensing agreement, this might effectively double your software costs.

Not only can moving to a DRaaS subscription reduce your hardware and software expenditures, it can lower your labor costs by moving the burden of maintaining the failover site to the vendor.

If you're considering third-party DRaaS solutions, you'll want to make sure that the vendor has the capacity for cross-regional multi-site backups. If a significant weather event like a hurricane impacted your primary office location, would the failover site be far enough away to remain unaffected by the storm? Also, would the vendor have adequate capacity to meet the combined needs of all its customers in your area if many were impacted at the same time? You're trusting your DRaaS vendor to meet RTOs and RPOs in times of crisis, so look for a service provider with a strong reputation for reliability.

Read "[Disaster Recovery as a Service \(DRaaS\) vs. Disaster Recovery \(DR\): Which Do You Need?](#)" for a comparative overview of both solutions.

What is DR? Business continuity planning Disaster recovery planning Disaster Re-

Report

Cost of a Data Breach Report 2024

Data breach costs have hit a new high. Get essential insights to help your security and IT teams better manage risk and limit potential losses.

[Read the report](#) →

Resources

Assessment

Cyber Resiliency

Assessment
Summary

Explore IBM Storage
Defender capabilities

The Cyber Resiliency Assessment is conducted through a no-cost, 2-hour virtual workshop with IBM ~~team~~ ~~experts~~ ~~capabilities~~ ~~provided~~ by IBM Storage Defender to help your organization build and deliver data resilience.

[Book a no-cost assessment](#)



[Read the summary](#)



Guide

Experience Desktop as a service on IBM Cloud

Empower your remote and hybrid workforce with Desktop as a service on IBM Cloud, achieving performance and security without compromise.

[Get the DaaS guide](#)



Webinar

The quickest way to protect sensitive data and ensure business continuity

Discover how IBM Storage Defender SaaS Essentials Edition can accelerate your approach to data resilience.

[Watch the webinar](#)



Webinar

Navigating the regulatory landscape and the impact on data protection and storage

Hear experts from IBM and Continuity Software discuss strategies for simplifying and accelerating your data resilience roadmap and the actions you should take to address the latest regulatory compliance requirements.

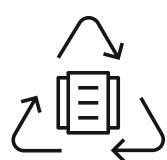
[Watch the webinar](#)



1 / 2

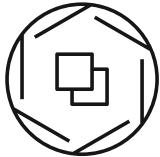


Related solutions



IBM Storage Defender

Protect your data from evolving threats no matter where it is stored with backup, AI-enabled threat detection and rapid recovery.

[Explore Storage Defender →](#)**Cloud disaster recovery solutions**

Protect your data with a cloud disaster recovery plan and mitigate the risk of downtime.

[Explore cloud disaster recovery →](#)**Storage data backup and recovery**

Accelerate enterprise backup and recovery processes to help retrieve data and recover IT services rapidly for on-premises and cloud workloads.

[Explore backup and recovery solutions →](#)

Take the next step

Keep your data safe and your workloads available with early threat detection, layers of protection and rapid recovery. Discover how IBM Storage Defender can help you protect your information supply chain.

[Explore Storage Defender →](#)[Book a live demo →](#)

