Recovery

KT2201 Recovering systems and disaster recovery

What is disaster recovery?

Disaster recovery (DR) is an organization's ability to respond to and recover from an event that negatively affects business operations. The goal of DR methods is to enable the organization to regain use of critical systems and IT infrastructure as soon as possible after a disaster occurs. To prepare for this, organizations often perform an in-depth analysis of their systems and create a formal document to follow in times of crisis. This document is known as a disaster recovery plan.

Read on to learn more about why DR is important, how it works, and the difference between disaster recovery and business continuity. You'll also discover what to include in a disaster recovery plan and the major types of DR, as well as major DR services and vendors.

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. Types of disaster include:

Cyber-attacks such as malware, DDoS and ransomware attacks

Sabotage

Power outages

Equipment failure

Epidemics or pandemics, such as COVID-19

Terrorist attacks or threats

Industrial accidents

Hurricanes

Tornadoes

Earthquakes

Floods

Fires

Why is disaster recovery important?

Disasters can inflict many types of damage with varying levels of severity, depending on the scenario. A brief network outage could result in frustrated customers and some loss of business to an e-commerce system. A hurricane or tornado could destroy an entire manufacturing facility, data centre or office.

Additionally, many businesses are required to create and follow plans for disaster recovery, business continuity and data protection in order to meet compliance regulations. This is particularly important for organizations operating in financial, healthcare, manufacturing and government sectors. Failure to have DR procedures in place can result in legal or regulatory penalties, so understanding how to comply with resiliency standards is important.

Preparing for every potential disaster may seem extreme, but the COVID-19 crisis illustrated that even scenarios that seem farfetched can come to pass. Businesses that had emergency measures in place to support remote work had a clear advantage when stay-at-home orders were enacted.

Thinking about disasters before they happen and creating a plan for how to respond can provide many benefits. It raises awareness about potential disruptions and helps an organization to prioritize its mission-critical functions. It also provides a forum for discussing these topics and making careful decisions about how to best respond in a low-pressure setting.

What is the difference between disaster recovery and business continuity?

On a practical level, DR and business continuity are often combined into a single corporate initiative and even abbreviated together as BCDR, but they are not the same thing. While the two disciplines have similar goals relating to an organization's resilience, they differ greatly in scope.

BC is a proactive discipline intended to minimize risk and help ensure the business can continue to deliver its products and services no matter the circumstances. It focuses especially on how employees will continue to work and how the business will continue operations while a disaster is occurring. BC is also closely related to business resilience, crisis management and risk management, but each of these has different goals and parameters.

DR is a subset of business continuity that focuses on the IT systems that enable business functions. It addresses the specific steps an organization must take to resume technology operations following an event. DR is also a reactive process by nature. While planning for it must be done in advance, DR activity is not kicked off until a disaster actually occurs.

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.

Understanding the difference between risk analysis and BIA and conducting the assessments can also help an organization define it goals when it comes to data protection and the need for backup. Organizations generally quantify these using measurements called recovery point objective (RPO) and recovery time objective (RTO).

Get started with your own analysis by reading our guide to BIA and free template.

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 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.

RPO and RTO are both important elements in disaster recovery, but the metrics have different uses. RPOs are acted on before a disruptive event takes place to ensure data will be backed up, while RTOs come into play after an event occurs.

Read more about calculating recovery objectives and the difference between RPO and RTO.

What's in a disaster recovery plan?

Once an organization has thoroughly reviewed its risk factors, recovery goals and technology environment, it can write a DR plan. The DR plan is the formal document that specifies these elements and outlines how the organization will respond when disruption or disaster occurs. The plan details recovery goals including RTO and RPO as well as the steps the organization will take to minimize the effects of the disaster.

The components of a DR plan should include:

A DR policy statement, plan overview and main goals of the plan.

Key personnel and DR team contact information.

A step-by-step description of disaster response actions immediately following an incident.

A diagram of the entire network and recovery site.

Directions for how to reach the recovery site.

A list of software and systems that staff will use in the recovery.

Sample templates for a variety of technology recoveries, including technical documentation from vendors.

A communication that includes internal and external contacts, as well as boilerplate for dealing with the media.

Summary of insurance coverage.

Proposed actions for dealing with financial and legal issues.

An organization should consider its DR plan a living document. Regular disaster recovery testing should be scheduled to ensure the plan is accurate and will work when a recovery is required. The plan should also be evaluated against consistent criteria whenever there are changes in the business or IT systems that could affect DR.

For more details and guidance, download a free DR plan template and planning guide.

How disaster recovery works

DR initiatives are more attainable by business of all sizes today due to widespread cloud adoption and availability of virtualization technologies that make backup and replication easier. However, much of the terminology and best practices developed for DR were based on enterprise efforts to recreate large-scale physical data centres. This involved plans to transfer, or fail over, workloads from a primary data centre to a secondary location or DR site in order to restore data and operations.

Disaster recovery sites

An organization uses a DR site to recover and restore its data, technology infrastructure and operations when its primary data centre is unavailable. DR sites can be internal, external or cloud-based.

An organization sets up and maintains an internal DR site. Organizations with large information requirements and aggressive RTOs are more likely to use an internal DR site, which is typically a second data centre. When building an internal site, the business must consider hardware configuration, supporting equipment, power maintenance, heating and cooling of the site, layout design, location and staff.

An external disaster recovery site is owned and operated by a third-party provider. External sites can be hot, warm or cold.

Hot site: A fully functional data centre with hardware and software, personnel and customer data, which is typically staffed around the clock and operationally ready in the event of a disaster.

Warm site: An equipped data centre that doesn't have customer data; an organization can install additional equipment and introduce customer data following a disaster.

Cold site: 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.

A cloud recovery site is another option. An organization should consider site proximity, internal and external resources, operational risks, service-level agreements and cost when contracting with cloud providers to host their DR assets or outsourcing additional services.

Disaster recovery tiers

In addition to choosing the most appropriate DR site, it may be helpful for organizations to consult the tiers of disaster recovery identified by the Share Technical Steering Committee and IBM in the 1980s. The tiers feature a variety of recovery options organizations can use as a blueprint to help determine the best DR approach depending on their business needs.

Another type of DR tiering involves assigning levels of importance to different types of data and applications and treating each tier differently based on the tolerance for data loss. This approach recognizes that some mission-critical functions may not be able to tolerate any data loss or downtime, while others can be offline for longer or have smaller sets of data restored.

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.

KT2202 Process for disaster recovery

What is Disaster Recovery?

How does disaster recovery work?

Disaster recovery relies upon the replication of data and computer processing in an off-premises location not affected by the disaster. When servers go down because of a natural disaster, equipment failure or cyber attack, a business needs to recover lost data from a second location where the data is backed up. Ideally, an organization can transfer its computer processing to that remote location as well in order to continue operations.

5 top elements of an effective disaster recovery plan

Disaster recovery team: This assigned group of specialists will be responsible for creating, implementing and managing the disaster recovery plan. This plan should define each team member’s role and responsibilities. In the event of a disaster, the recovery team should know how to communicate with each other, employees, vendors, and customers.

Risk evaluation: Assess potential hazards that put your organization at risk. Depending on the type of event, strategize what measures and resources will be needed to resume business. For example, in the event of a cyber attack, what data protection measures will the recovery team have in place to respond?

Business-critical asset identification: A good disaster recovery plan includes documentation of which systems, applications, data, and other resources are most critical for business continuity, as well as the necessary steps to recover data.

Backups: Determine what needs backup (or to be relocated), who should perform backups, and how backups will be implemented. Include a recovery point objective (RPO) that states the frequency of backups and a recovery time objective (RTO) that defines the maximum amount of downtime allowable after a disaster. These metrics create limits to guide the choice of IT strategy, processes and procedures that make up an organization’s disaster recovery plan. The amount of downtime an organization can handle and how frequently the organization backs up its data will inform the disaster recovery strategy.

Testing and optimization: The recovery team should continually test and update its strategy to address ever-evolving threats and business needs. By continually ensuring that a company is ready to face the worst-case scenarios in disaster situations, it can successfully navigate such challenges. In planning how to respond to a cyber attack, for example, it’s important that organizations continually test and optimize their security and data protection strategies and have protective measures in place to detect potential security breaches.

KT2203 Expecting things to go wrong

Most Common Computer Problems

The Computer Won't Start. A computer that suddenly shuts off or has difficulty starting up could have a failing power supply. ...

The Screen is Blank. ...

Abnormally Functioning Operating System or Software. ...

Windows Won't Boot. ...

The Screen is Frozen. ...

Computer is Slow. ...

Strange Noises. ...

Slow Internet.

KT2204 Using boot logs to troubleshoot problems

Create a boot log for troubleshooting

Problems that you're troubleshooting in Windows XP often originate in the boot process. As such, one of your key troubleshooting techniques should be to create a boot log. Creating such a log is a relatively easy process. Follow these steps: Restart the system. When the operating system begins to load, press [F8]. Select the Enable ...

Problems that you're troubleshooting in Windows XP often originate in the boot process. As such, one of your key troubleshooting techniques should be to create a boot log. Creating such a log is a relatively easy process.

Follow these steps:

Restart the system.

When the operating system begins to load, press [F8].

Select the Enable Boot Logging option from the Windows Advanced menu, and press [Enter].

After the system restarts, launch Notepad, and open the C:\Windows\Ntbtlog.txt file. This file contains a list of all of the files that Windows XP attempted to load during startup.

Every line in the file will begin with either "Loaded driver" or "Did not load driver," which makes it easy to determine what drivers or services could be causing the problem. In either case, the path and filename of the driver or service will follow.

KT2205 Process for booting a system into safe mode

The Advanced Boot Options screen lets you start Windows in advanced troubleshooting modes. You can access the menu by turning on your computer and pressing the F8 key before Windows starts.

Some options, such as safe mode, start Windows in a limited state, where only the bare essentials are started. If a problem doesn't reappear when you start in safe mode, you can eliminate the default settings and basic device drivers and services as possible causes. Other options start Windows with advanced features intended for use by system administrators and IT professionals. For more information, go to the Microsoft website for IT professionals.

Repair Your Computer

Shows a list of system recovery tools you can use to repair startup problems, run diagnostics, or restore your system. This option is available only if the tools are installed on your computer's hard disk. If you have a Windows installation disc, the system recovery tools are located on that disc.

Safe Mode

Starts Windows with a minimal set of drivers and services.

To start in safe mode:

Remove all floppy disks, CDs, and DVDs from your computer, and then restart your computer. Click the Start button, click the arrow next to the **Shut Down** button (or the arrow next to the **Lock** button), and then click **Restart**.

Do one of the following:

If your computer has a single operating system installed, press and hold the F8 key as your computer restarts. You need to press F8 before the Windows logo appears. If the Windows logo appears, you'll need to try again by waiting until the Windows logon prompt appears, and then shutting down and restarting your computer.

If your computer has more than one operating system, use the arrow keys to highlight the operating system you want to start in safe mode, and then press F8.

On the **Advanced Boot Options** screen, use the arrow keys to highlight the safe mode option you want, and then press Enter.

Log on to your computer with a user account that has administrator rights.

Safe Mode with Networking. Starts Windows in safe mode and includes the network drivers and services needed to access the Internet or other computers on your network.

Safe Mode with Command Prompt. Starts Windows in safe mode with a command prompt window instead of the usual Windows interface. This option is intended for IT professionals and administrators.

Enable Boot Logging. Creates a file, ntbtlog.txt, that lists all the drivers that are installed during startup and that might be useful for advanced troubleshooting.

Enable low-resolution video (640×480). Starts Windows using your current video driver and using low resolution and refresh rate settings. You can use this mode to reset your display settings. For more information, see Change your screen resolution.

Last Known Good Configuration (advanced). Starts Windows with the last registry and driver configuration that worked successfully.

Directory Services Restore Mode. Starts Windows domain controller running Active Directory so that the directory service can be restored. This option is intended for IT professionals and administrators.

Debugging Mode. Starts Windows in an advanced troubleshooting mode intended for IT professionals and system administrators.

Disable automatic restart on system failure. Prevents Windows from automatically restarting if an error causes Windows to fail. Choose this option only if Windows is stuck in a loop where Windows fails, attempts to restart, and fails again repeatedly.

Disable Driver Signature Enforcement. Allows drivers containing improper signatures to be installed.

Start Windows Normally. Starts Windows in its normal mode.

KT2206 Emergency repair

Short for **Emergency Repair Disk**, an **ERD** is a diskette that creates backups of system files and settings and helps troubleshoot and fix issues for Windows NT and Windows 2000 users. The ERD is used in conjunction with the Windows repair option and prompts for the diskette when needed. Note: The ERD is not to be confused with a standard boot diskette as it cannot be used alone.

ERD capabilities

Verifying the boot sector is not corrupt.

Repairing any start up files.

Locate any missing or damaged system files.

KT2207 Factory repair partitions

What is a recovery partition?

Due to the inclusion on their PC by default, many users assume the recovery partition isn't something they should mess with. In reality, though, it's completely safe and relatively easy to format the OEM recovery partition and create a recovery partition of your own.

The recovery partition is simply a save of the system's state when the manufacturer first set up the PC. It usually takes the form of a .wim file that can be accessed through the usual recovery interface. You can create a recovery partition in Windows yourself to replace those files, but it's usually not a good idea to simply delete the OEM partition without replacing it.

To create a recovery drive in Windows 10, you must first create a Windows recovery image, before preparing the partition and adding it to your boot menu for easy access. If you want to create a full Windows 10 System Image Backup, there is an easier way to do it which does not work to update the recovery partition.

How to Capture a Windows Recovery Image as a WIM file

There's some preparation required before you create your windows recovery image, though this is reduced if you already keep your OS maintained and up-to-date. First, make sure your PC is fully updated, has the user accounts and software you want to be included, and has the themes/settings you'd prefer. Once complete, boot from Windows installation media by following this guide.

Open Command Prompt via Windows Installation Media

Once your PC boots, ignore the setup screen and press “Shift + F10” to open the command-line interface.

(Optional) Initialize networking services