By its very nature, a *disaster recovery plan* is implemented only when tension is high and cooler heads may not naturally prevail. Picture the circumstances in which you might find it necessary to implement DRP measures—a hurricane destroys your main operations facility; a fi re devastates your main processing center; terrorist activity closes off access to a major metropolitan area. Any event that stops, prevents, or interrupts an organization’s ability to perform its work tasks is considered a disaster. The moment that IT becomes unable to support mission-critical processes is the moment DRP kicks in to manage the restoration and recovery procedures.

**Natural Disasters**

**Fault tolerance** is the ability of a system to suffer a fault but continue to operate. Fault tolerance is achieved by adding redundant components such as additional disks within a redundant array of inexpensive disks (RAID) array. Fault tolerance is not the same as a backup

**System resilience** refers to the ability of a system to maintain an acceptable level of service during an adverse event. This could be a hardware fault managed by fault-tolerant components, or it could be an attack managed by other controls such as effective intrusion detection and prevention systems. In some contexts, it refers to the ability of a system to return to a previous state after an adverse event. For example, if a primary server in a failover cluster fails, fault tolerance ensures that the system fails over to another server. System resilience implies that the cluster can fail back to the original server after the original server is repaired.

**Manual Recovery** If a system fails, it does not fail in a secure state. Instead, an administrator is required to manually perform the actions necessary to implement a secured or trusted recovery after a failure or system crash

**Automated Recovery** The system is able to perform trusted recovery activities to restore itself against at least one type of failure. For example, a hardware RAID provides automated recovery against the failure of a hard drive but not against the failure of the entire server. Some types of failures will require manual recovery.

**Automated Recovery without Undue Loss** This is similar to automated recovery in that a system can restore itself against at least one type of failure. However, it includes mechanisms to ensure that specific objects are protected to prevent their loss. A method of automated recovery that protects against undue loss would include steps to restore data or other objects. It may include additional protection mechanisms to restore corrupted fi les, rebuild data from transaction logs, and verify the integrity of key system and security components.

**Function Recovery** Systems that support function recovery are able to automatically recover specific functions. This state ensures that the system is able to successfully complete the recovery for the functions, or that the system will be able to roll back the changes to return to a secure state.

**Quality of Service**

Quality of service (QoS) controls protect the integrity of data networks under load. Many different factors contribute to the quality of the end-user experience, and QoS attempts to manage all of those factors to create an experience that meets business requirements. Some of the factors contributing to QoS are as follows:

**Bandwidth** The network capacity available to carry communications.

**Latency** The time it takes a packet to travel from source to destination.

**Jitter** The variation in latency between different packets.

**Packet Loss** Some packets may be lost between source and destination, requiring retransmission.

Interference Electrical noise, faulty equipment, and other factors may corrupt the contents of packets.

Recovery Strategy

**Crisis Management**

**Emergency Communications**

**Workgroup Recovery**

To facilitate this effort, it’s sometimes best to develop separate recovery facilities for different workgroups. For example, if you have several subsidiary organizations that are in different locations and that perform tasks similar to the tasks that workgroups at your office perform, you may want to consider temporarily relocating those workgroups to the other facility and having them communicate electronically and via telephone.

**Alternate Processing Sites**

One of the most important elements of the disaster recovery plan is the selection of alternate processing sites to be used when the primary sites are unavailable. Many options are available when considering recovery facilities, limited only by the creative minds of disaster recovery planners and service providers.

**Cold Sites**

Cold sites are standby facilities large enough to handle the processing load of an organization and equipped with appropriate electrical and environmental support systems. They may be large warehouses, empty office buildings, or other similar structures. However, a cold site has no computing facilities (hardware or software) preinstalled and also has no active broadband communications links. Many cold sites do have at least a few copper telephone lines, and some sites may have standby links that can be activated with minimal notification. The time to activate a cold site is often measured in weeks,

**Hot Sites**

A hot site is the exact opposite of the cold site. In this configuration, a backup facility is maintained in constant working order, with a full complement of servers, workstations, and communications links ready to assume primary operations responsibilities. The servers and workstations are all preconfigured and loaded with appropriate operating system and application software.

**Warm Sites**

Warm sites occupy the middle ground between hot and cold sites for disaster recovery specialists. They always contain the equipment and data circuits necessary to rapidly establish operations. As with hot sites, this equipment is usually preconfigured and ready to run appropriate applications to support an organization’s operations. Unlike hot sites, however, warm sites do not typically contain copies of the client’s data. The main requirement in bringing a warm site to full operational status is the transportation of appropriate backup media to the site and restoration of critical data on the standby servers. Activation of a warm site typically takes at least 12 hours from the time a disaster.

**Mobile Sites**

Mobile sites are nonmainstream alternatives to traditional recovery sites. They typically consist of self-contained trailers or other easily relocated units. These sites include all the environmental control systems necessary to maintain a safe computing environment. Larger corporations sometimes maintain these sites on a “fly-away” basis, ready to deploy them to any operating location around the world via air, rail, sea, or surface transportation. Mobile sites are usually configured as cold sites or warm sites,

**Service Bureaus**

A service bureau is a company that leases computer time. Service bureaus own large server farms and often fields of workstations. Any organization can purchase a contract from a service bureau to consume some portion of their processing capacity. Access can be on site or remote.

**Cloud Computing**

Many organizations now turn to cloud computing as their preferred disaster recovery option. Infrastructure as a Service (IaaS) providers, such as Amazon Web Services, Microsoft Azure, and Google Compute Cloud, offer on-demand service at low cost. Companies wishing to maintain their own datacenters may choose to use these IaaS options as backup service providers.

**Mutual Assistance Agreements**

*Mutual assistance agreements* (MAAs), also called *reciprocal agreements,* are popular in disaster recovery literature but are rarely implemented in real-world practice. In theory, they provide an excellent alternate processing option. Under an MAA, two organizations pledge to assist each other in the event of a disaster by sharing computing facilities or other technological resources. They appear to be extremely cost effective at

first glance.

**Electronic Vaulting**

In an electronic vaulting scenario, database backups a g re moved to a remote site using bulk transfers. The remote location may be a dedicated alternative recovery site (such as a hot site) or simply an offsite location managed within the company or by a contractor for the purpose of maintaining backup data. If you use electronic vaulting, remember that there may be a significant delay between the time you declare a disaster and the time your database is ready for operation with current data. If you decide to activate a recovery site, technicians will need to retrieve the appropriate backups from the electronic vault and apply them to the soon-to-be production servers at the recovery site.

**Remote Journaling**

With remote journaling , data transfers are performed i g n a more expeditious manner. Data transfers still occur in a bulk transfer mode, but they occur on a more frequent basis, usually once every hour and sometimes more frequently. **Unlike electronic vaulting scenarios, where entire database backup fi les are transferred, remote journaling setups transfer copies of the database transaction logs** containing the transactions that occurred since the previous bulk transfer.

**Remote Mirroring**

Remote mirroring is the most advanced database backup solution. Not surprisingly, it’s also the most expensive! Remote mirroring goes beyond the technology used by remote journaling and electronic vaulting; with remote mirroring, a live database server is maintained at the backup site. The remote server receives copies of the database modifications at the same time they are applied to the production server at the primary site. Therefore, the mirrored server is ready to take over an operational role at a moment’s notice .

Recovery Plan Development

Executive summary providing a high-level overview of the plan

■ Department-specific plans

■ Technical guides for IT personnel responsible for implementing and maintaining critical backup systems

■ Checklists for individuals on the disaster recovery team

■ Full copies of the plan for critical disaster recovery team members

**Assessment**

**Backups and Offsite Storage**

**Backup Tape Formats**

The physical characteristics and the rotation cycle are two factors that a worthwhile backup solution should track and manage. The physical characteristics involve the type of tape drive in use. This defines the physical wear placed on the media. The rotation cycle is the frequency of backups and retention length of protected data. By overseeing these characteristics, you can be assured that valuable data will be retained on serviceable backup media. Backup media has a maximum use limit; perhaps 5, 10, or 20 rewrites may be made before the media begins to lose reliability (statistically speaking). A wide variety of backup tape formats exist:

■ Digital Data Storage (DDS)/Digital Audio Tape (DAT)

■ Digital Linear Tape (DLT) and Super DLT

■ Linear Tape Open (LTO)

**Disk-to-Disk Backup**

Over the past decade, disk storage has become increasingly inexpensive. With drive capacities now measured in terabytes (TB), tape and optical media can’t cope with data volume requirements anymore. Many enterprises now use disk-to-disk (D2D) backup solutions for some portion of their disaster recovery strategy.

One important note: Organizations seeking to adopt an entirely disk-to-disk approach must remember to maintain geographical diversity. Some of those disks have to be located offsite. Many organizations solve this problem by hiring managed service providers to manage remote backup locations.

**Tape Rotation**

There are several commonly used tape rotation strategies for backups: The Grandfather- Father-Son (GFS) strategy, the Tower of Hanoi strategy, and the Six Cartridge Weekly Backup strategy. These strategies can be fairly complex, especially with large tape sets. **They can be implemented manually using a pencil and a calendar or automatically by using either commercial backup software or a fully automated hierarchical storage management (HSM) system**. **An HSM system is an automated robotic backup jukebox consisting of 32 or 64 optical or tape backup devices. All the drive elements within an HSM system are configured as a single drive array (a bit like RAID).**

**Software Escrow Arrangements**

A software escrow arrangement is a unique tool used to protect a company against the failure of a software developer to provide adequate support for its products or against the possibility that the developer will go out of business and no technical support will be available for the product.

**Read-Through Test**

The read-through test is one of the simplest tests to conduct, but it’s also one of the most critical. In this test, you distribute copies of disaster recovery plans to the members of the disaster recovery team for review. This lets you accomplish three goals simultaneously:

■ It ensures that key personnel are aware of their responsibilities and have that knowledge refreshed periodically

It provides individuals with an opportunity to review the plans for obsolete information and update any items that require modification because of changes within the organization.

■ In large organizations, it helps identify situations in which key personnel have left the company and nobody bothered to reassign their disaster recovery responsibilities. This is also a good reason why disaster recovery responsibilities should be included in job descriptions.

**Structured Walk-Through**

A structured walk-through takes testing one step further. In this type of test, often referred **to as a table-top exercise , members of the disaster recovery team gather in a large conference room and role-play a disa**ster scenario. Usually, the exact scenario is known only to the test moderator, who presents the details to the team at the meeting. The team members then refer to their copies of the disaster recovery plan and discuss the appropriate responses to that particular type of disaster.

**Simulation Test**

Simulation tests are similar to the structured walk-throughs. In simulation tests, disaster recovery team members are presented with a scenario and asked to develop an appropriate response. Unlike with the tests previously discussed, some of these response measures are then tested. This may involve the interruption of noncritical business activities and the use of some operational personnel

**Parallel Test**

Parallel tests represent the next level in testing and involve relocating personnel to the alternate recovery site and implementing site activation procedures. The employees relocated to the site perform their disaster recovery responsibilities just as they would for an actual disaster. The only difference is that operations at the main facility are not interrupted. That site retains full responsibility for conducting the day-to-day business of the organization.

**Full-Interruption Test**

Full-interruption tests operate like parallel tests, but they involve actually shutting down operations at the primary site and shifting them to the recovery site. For obvious reasons, full-interruption tests are extremely difficult to arrange, and you often encounter resistance from management.

**Maintenance**

Remember that a disaster recovery plan is a living document. As your organization’s needs change, you must adapt the disaster recovery plan to meet those changes.

The Electronic Discovery Reference Model consists of nine steps for electronically stored information ([ESI](https://searchcompliance.techtarget.com/definition/electronically-stored-information-ESI)) management.

Information management: Implement [data governance](https://searchcompliance.techtarget.com/definition/information-governance) processes that alleviate risk and expenses in the event of an electronic discovery request.

Identification: Locate sources of information to determine exactly what the data is, and how it needs to be managed.

Preservation: Ensure potentially e-discovery-relevant ESI is properly stored using measures such as retention and deletion schedules.

Collection: Gather information for e-discovery use.

Processing: Reduce the volume the relevant ESI and convert it for review and analysis.

Review: Determine the data's e-discovery relevance.

Analysis: Evaluate the ESI for content and context, including key patterns and topics.

Production: Deliver the ESI to relevant parties.

Presentation: Display [data](https://searchdatamanagement.techtarget.com/definition/data) findings at depositions, hearings, trials, etc., to elicit further information, validate existing facts or positions or persuade a jury…