Disaster recovery (DR) plans need to be flexible and scalable to address a broad range of disruption scenarios. The same goes for business continuity (BC) plans. Both plans also need to be tested regularly to ensure that the technology, processes and people all work together with as minimal disruption to the business as possible when a disaster strikes.

This data center disaster recovery planning guide focuses on best practices for [setting up a DR plan](https://www.techtarget.com/searchdisasterrecovery/tip/Disaster-recovery-plan-checklist-Identifying-weak-points-in-your-plan). Discover the most important factors in a successful data center DR plan, who should be involved in the planning process and how to get started.

**What's the difference between business continuity plans and disaster recovery plans?**

Business continuity plans ensure people have a place to work when their original location becomes unusable. A BC plan should outline essential business functions, clearly identify those systems and processes that must operate without interruption, and specify [how to maintain them](https://searchservervirtualization.techtarget.com/tip/Build-an-IT-maintenance-plan-around-infrastructure-needs). It should take into account any possible business disruption.

A DR plan is a broad term that describes a process to recover disrupted IT systems, networks and other critical assets an organization uses. Having a DR site is a crucial factor when planning your organization's recovery from any disaster.

Companies can set up an internal site that it owns and manages, or an external site through a cloud or service provider. Organizations that need data back quickly often choose an internal site, typically a second data center that enables quick resumption of business. However, [cloud-based disaster recovery](https://www.techtarget.com/searchcloudcomputing/photostory/252469890/6-steps-to-survive-a-cloud-outage/1/Prepare-for-a-cloud-outage) options increasingly offer fast response times to meet tight recovery time objectives.

External DR sites can be hot, warm or cold. A hot site can serve as a fully functional data center that companies can move into if a disaster hits the primary data center. A warm site has equipment, but not data. The organization must add customer data -- and often hardware and software -- after the disaster strikes. A cold site has IT infrastructure, but no equipment until a disaster hits. Cold sites are for organizations or specific workloads that can wait for an extended period to get back up and running.

An organization may use several types of sites, putting its most critical applications and data in a hot site and less important systems in warm or cold sites.



For comparison purposes, a data center disaster recovery plan focuses exclusively on a data center facility and its infrastructure, e.g., physical location, construction, security, power sources and environmental systems.

**First steps: An operational risk assessment**

A key activity in preparing a data center DR plan is an [*operational risk assessment*](http://siteresources.worldbank.org/EXTFINANCIALSECTOR/Resources/282884-1239831335682/6028531-1239831365859/G-Operational_Risk_Assessment-Fulton.pdf) of the building or facility. The assessment analyzes key operating components, such as building location, e.g., access routes, proximity to fuel storage tanks, proximity to highways, rail lines and airports; power generation, e.g., commercial power, backup power systems; power protection, e.g., grounding and bonding, lightning arrestors, line conditioners, surge suppressors; HVAC (heating, ventilation and air conditioning); critical systems, e.g., servers, VoIP systems; network infrastructure, e.g., cabling, connectors, routers, copper and fiber circuits; security, e.g., physical access and information security; workspace, e.g., offices, conference rooms, cubicles, furniture, lighting; fire protection, e.g., fire detectors, smoke detectors, fire extinguishers, FM-200 extinguishing systems; building floors and walls, e.g., fire-rated walls, raised floors; and utilities, e.g., water, power, sewer, communications.

When planning a data center operations risk assessment, coordinate with IT management and building management, if your firm is a tenant, or with facilities management, if you own the building. Review your objectives for the assessment with these organizations before starting.

And review your risk assessment checklist -- if you have one -- with IT management, building management and facilities management to ensure you cover all the bases. If possible, ask IT and facilities for any assessments they conducted or have on file. These may help save you time, unless the data is more than a year old.

Perform the following actions in the assessment:

1. The data center DR plan development team should meet with various IT groups, such as the internal technology team, application team and network administrator(s). This ensures all the groups that regularly use the data center's facilities have input into the [DR planning process](https://www.techtarget.com/searchdisasterrecovery/feature/Top-5-disaster-recovery-and-planning-questions-asked-in-2019).
2. List internal and external data center assets, third-party suppliers and resources, and other stakeholders.
3. Gather all relevant infrastructure documents, e.g., building plans, floor plans, system maps, network diagrams and equipment configurations.
4. If it's available, obtain a copy of the existing data center DR plan. If this does not exist, proceed with the following steps:
   1. Work with management to find out the most serious threats to the data center, e.g., fire, human error, loss of power, system failure, security breach.
   2. Work with management to discover the most serious vulnerabilities to the data center, e.g., outdated backup power systems.
   3. Review the history of data center outages and disruptions and how they were handled.
   4. Determine the maximum outage time management can accept if the data center is unavailable.
   5. Identify current procedures for responding to data center disruptions.
   6. Determine when these procedures were last tested.
   7. Identify data center emergency team(s). Determine their level of training with regard to emergencies.
   8. Identify data center vendor emergency response capabilities, specifically if they have ever been used, if they worked properly, the cost of the services and the status of service contracts.

Compile the results from data center operational assessments into a gap analysis report that identifies what is currently done versus what ought to be done, with recommendations on how to achieve the required level of preparedness and the estimated investment required.

As part of the analysis process, examine the impact of a data center disruption on the business. What will happen to critical business processes if data center operations are disrupted? What might happen to the company's image, reputation and competitive position in the aftermath of a data center disruption?

In addition to identifying business impacts, the assessment can demonstrate opportunities for improvement, and it can also help the development of the DR plan by identifying existing situations -- e.g., older diesel generator that should be replaced -- that may be affected by a disruption.

**Developing a data center disaster recovery plan**

Once you have analyzed the data center and have identified potential risks to operations, prioritize the risk scenarios in order of severity, potential damage and likelihood of occurrence. This can be used to focus the plan's response activities in the proper sequence for the situation. (see our [**free, downloadable DR planning template and checklist**](https://www.techtarget.com/searchdisasterrecovery/pro/Data-Center-DR-Plan-Template?Offer=Content_OTHR-Edit_OTHR-Template_11/24/2020_DRPlanTemplate))



Using the structure noted in the National Institute of Standards and Technology's SP 800-34 standard, "Contingency Planning Guide for Information Technology Systems," we can expand those activities into the following structured sequence of activities:

1. The data center plan development team should meet with the internal technology team, facilities department, utility service providers and relevant vendors to establish the scope of the activity, e.g., internal and external threats, internal and external assets, third-party resources, and linkages to other offices/clients/vendors. Be sure to brief senior management on these meetings so they are properly informed.
2. Gather all relevant infrastructure documents, e.g., building floor plans, building site plans, utility diagrams, HVAC diagrams, network diagrams and equipment configurations.
3. Obtain copies of existing [IT disaster recovery plans](https://www.techtarget.com/searchdisasterrecovery/feature/IT-disaster-recovery-DR-plan-template-A-free-download-and-guide). If these do not exist, proceed with the following steps:
   1. Work with management to determine the most serious threats to the data center infrastructure, e.g., fire, human error, loss of power, flooding, system failure, severe weather.
   2. Identify what management perceives as the most serious vulnerabilities to the data center, e.g., insufficient backup power, minimal building security, proximity of the data center to a flood plain.
   3. Review the history of data center outages and disruptions and how the firm handled them.
   4. Identify what management perceives as the most critical data center assets, e.g., server farms, storage systems, network infrastructure, staffing.
   5. Determine the maximum outage time management can accept if the identified data center assets are unavailable.
   6. Identify the operational procedures currently used to respond to critical data center outages.
   7. Determine when these procedures were last tested to validate their relevance.
   8. Identify emergency response team(s) for all critical data center disruptions. Determine their level of training, especially in emergencies.
   9. Identify vendor emergency response capabilities: if they have ever been used; if they were, if they worked properly; how much the company is paying for these services; the status of data center maintenance contracts; the [presence of service-level agreement(s)](https://www.techtarget.com/searchitchannel/definition/service-level-agreement) if used.
4. Compile results from all the assessments into a gap analysis report that identifies what is currently done versus what ought to be done, with recommendations as to how to achieve the required level of data center preparedness, and the investment required.
5. Have management review the report and agree on the recommended actions.
6. Prepare data center disaster recovery plan(s) to address critical assets, e.g., hardware and software, data storage, networks.
7. Conduct tests of plans and system recovery assets to validate their operation.
8. Update data center DR plan documentation to reflect changes.
9. Schedule next review/audit of data center disaster recovery capabilities.

**Important data center disaster recovery plan caveats**

When building a data center DR plan, keep in mind the following guidance:

* Obtain senior management support so your plans can be funded.
* Take the data center DR planning process seriously: Plans don't have to be dozens of pages long; rather, they need the right information, and that information should be current and accurate.
* Consider using standards as part of the process, including NIST SP 800-34, [ISO/IEC 24762:2008](http://www.iso.org/iso/catalogue_detail.htm?csnumber=41532) and BS 25777:2008, as they provide a useful structured format for plans, as well as guidance on the issues to address. This aspect is particularly important if plans will be audited.
* Keep the planning process simple by gathering and organizing accurate information.
* Review results with key departments, such as IT and facilities, to ensure your assumptions are correct.

Data center disaster plans help protect a significant investment for most organizations. While some firms address data center recovery by building a second data center or leasing specially equipped space at a third-party facility, a careful assessment of data center operations and risks is an important starting point in a DR program.