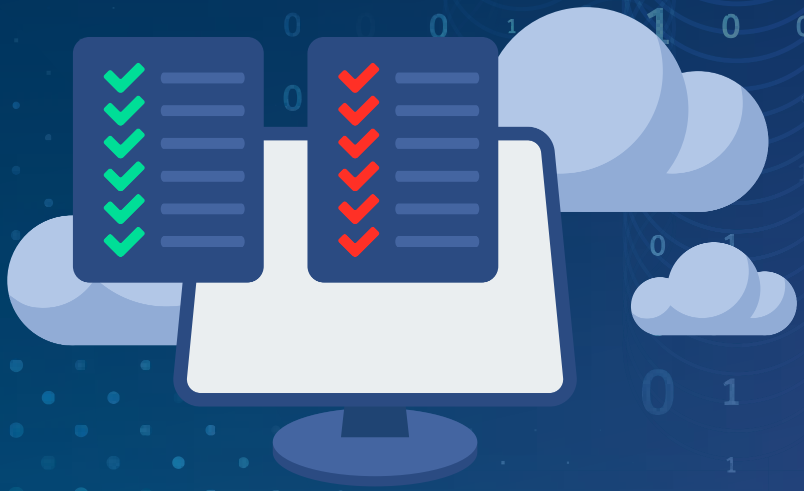


BUSINESS CONTINUITY PLAN vs DISASTER RECOVERY PLAN:

ALL YOU NEED TO KNOW

Business continuity and **disaster recovery planning** are mandatory nowadays, as they help Managed Service Providers (MPSs) and their clients stay afloat and tackle any business interruption generated by artificial or natural disasters. Still, creating the actual plans isn't enough to maintain business operations. You need to understand what each plan needs to cover, the key difference between the disaster recovery process and business continuity planning, and how to manage risk and keep business operations going.

This eBook will walk you through everything you need to know about maintaining business continuity and performing disaster recovery planning, so your organization resumes its normal operations in record time.

What is a business continuity plan?

A business continuity plan (BCP) is a document that details the course of action that an organization needs to follow to resume critical processes if a disaster, such as a calamity, a cyberattack, or a power outage, occurs. This way, companies ensure their people and assets are protected in an emergency, that communications between employees and customers are supported, normal business operations are quickly restored, and data is secured.

Since business continuity planning is crucial for solid businesses, it takes careful consideration and work. Business continuity plans are based on clearly defining all the risks that may affect the organization’s critical business functions. Once this is done, you should assess each risk individually to showcase how it impacts work and can be mitigated. After this, the business continuity plan should be tested and reviewed so that you may correct any weaknesses. When this whole process is over, your company and your MSP should have a bullet-proof BCP.

What is a disaster recovery plan?

A disaster recovery plan (DRP) ensures that the business remains operational and that you may still accomplish business objectives during disruptions. A disaster recovery plan showcases how you can fully recover all critical data, IT systems, and networks in an emergency by providing a well-documented approach.

The DR plan document details the list of actions the company's team must take before, during, and after a natural disaster or an artificial one. Activities like terrorism attempts, hacking, technical glitches, system failures, or human errors can cost tens of thousands to millions, depending on their complexity and the company's size.

Business continuity vs disaster recovery plan: What are their similarities and key differences?

Business continuity and disaster recovery are proactive strategies based on risk assessment and are meant to make business operational in case a catastrophic event occurs.

While both have a relevant crisis management component and business continuity and disaster recovery plans complement one another, they have different objectives. Business continuity focuses on keeping critical business processes running, ensuring a company provides its vital functions, even with minimal resources or in a different location. The Disaster Recovery Plan focuses on restoring activity to normal.

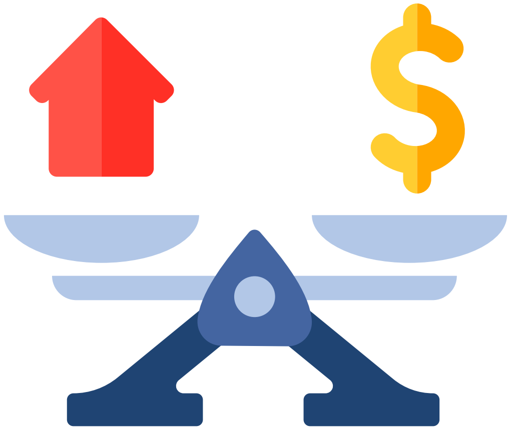
In this context, the key performance indicators required to assess the efficiency of each plan are different.

→ **One key priority of business continuity planning is ensuring that phones, emails, or network servers work, so that company members may still communicate with clients and partners to inform them of specific issues and delays or ask for support.**

→ **Effective disaster recovery plans could include employee safety measures, such as purchasing emergency supplies or conducting fire drills.**

→ **Since business continuity planning differentiates itself from disaster recovery planning, even the two dedicated teams work separately. As the business continuity people apply one or several contingency plans, the disaster recovery ones work to reinstate the original facilities and restore business processes.**

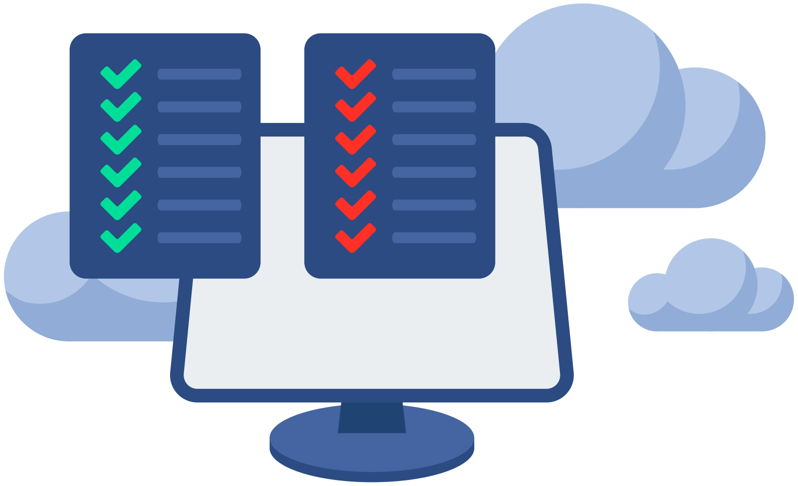
Some companies treat disaster recovery plans as a part of their business continuity strategy, which is fine as long as the priorities are clear.



Importance of planning for business continuity, disaster recovery, or both

Sometimes underestimating the importance of planning for business continuity and disaster recovery is understandable. With so many daily activities and operational issues to solve, preparing for something that might never happen seems like a waste of time and resources. The only aspect is that when a disaster scenario occurs, the absence of business continuity plans and disaster recovery plans can have business-ending consequences. An unplanned interruption of business generates chaos in many companies. If no business continuity or disaster recovery strategy is in place, it's impossible to identify and implement the best solutions on the spot. This causes revenue drops for the organization and significantly impacts its reputation and relationship with stakeholders.

If we take into account the unexpected issues with which the modern world has been dealing in the past years – pandemics, wars, energy crises, cyber-attacks, and terrorism threats – we can agree that having both a business continuity and a disaster recovery plan is mandatory, for any company that wants to make it.



Apart from providing structure in an unforeseen critical event, where many variables exist, business continuity plans and disaster recovery plans are essential for several reasons:

BC and DR plans allow your employees to continue business operations and deliver

Business continuity and disaster recovery plans protect your business and employees. The fact that some of them can still perform their tasks and that everyone can get back to work, as soon as possible, means that they will still earn a salary, which is highly appreciated in times of distress. Your MSP will cater to your company's needs for resuming business operations, to keep your business running.

BC and DR plans reduce costs associated with downtime

According to the Uptime Institute's 2022 Outage Analysis Report, 80% of data center managers and operators have experienced outages between 2019-2022. 60% of outages generated costs of $100,000 per company, while 15% drove losses of $1 million.

Still, things don't stop here. The cost of downtime increases when we talk about industries more prone to risks, such as banking and finance, governmental organizations, healthcare, manufacturing, media, and communications. In the worst cases, downtime can be as costly as $5 million per hour, as ITIC research points out.

By ensuring you have a business continuity and a disaster recovery plan for minimal disruption, this will limit your organization's unrealized incomes.

A guide to disaster recovery planning

Planning for disaster recovery implies compiling crucial information and procedures into DRP and sharing it with your DR team. The essential steps you need to take to develop the plan are the following:

1. **Define what you have**

   Start your disaster recovery plan by assessing its scope and the funding available. When the management approves a budget, you can put together a list of actions with your MSP.

   Make a list of your step-by-step procedures for recovery of all physical, mechanical, and virtual items and those for alerting key people, such as staff members, family members, vendors, clients, and stakeholders.

   Lastly, a training process should walk the DRP team through all these.

2. **Identify key elements**

   Defining your IT infrastructure and resources is essential in disaster recovery planning. Then, your MSP can continue with the risk identification process and procedures for replacing equipment and for obtaining spare parts. A designated spokesperson from your MSP will update your team on needs and quantities.

3. **Determine objectives and procedures**

   Next, it is time to focus on your key performance indicators and disaster recovery strategies. Firstly, your organization should determine the target Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

   The RTO is when the business needs to restore vital systems without incurring significant operational downtime and outages. The RPO is the data loss tolerance, also known as the amount of data a company can lose compared to the last backup.

   Your MSP uses a best-in-class recovery point objective (RPO) of 15-minutes and a recovery time objective (RTO) of less than 1-hour.

   Then comes the response and recovery strategies, the event notification procedures (that may be automated or outsourced), the recovery failover procedures, the failback procedures, and, after everything has been concluded, the resumption of business procedures.

   These parts of your plan need to consider sensitive questions, like “will you pay a ransom?”

4. **Use hot or cold sites (if applicable)**

   Depending on the type of disaster, your company might need to use hot or cold sites. Hot sites include the hardware, software, servers, and computers necessary to keep business running, while cold sites only provide the power, the environment, and the workspaces. This can be discussed with your MSP.

The steps to business continuity planning

When it comes to creating a business continuity plan, there are several steps that we recommend considering:

1. **Create a Business Continuity Management Team**
   Effective business continuity plans start with defining the business continuity management team. The best way to ensure everyone knows what is expected of them is to provide descriptions of the roles and responsibilities.

   Then, you have to add each business continuity team member's contact details to a company-wide available list and set up a process for implementing the business continuity plan and how you will communicate each step to the team.

2. **Prioritize employee safety**
   The first aspect you need to focus on when creating business continuity plans is your employees' safety. At this stage, you have to consider whether your company is prepared for remote access, whether additional safety measures and equipment are required for those who can't work remotely (e.g., protective masks), and whether you

can remain flexible by reallocating resources and reorganizing teams.

Since a difficult situation might drive concern among team members, it’s essential to keep them in the loop by giving them constant updates and following a communications schedule. A good solution would be to use business continuity software and integrated messaging tools that enable people to communicate with one another. Your MSP can advice you on tools.

3. **Assess your company’s risks**

   Your business continuity management team is responsible for working with your MSP to conduc a business impact analysis (BIA) that identifies threats specific to your industry and company. For each scenario, you should understand how it could impact your business operations in depth.

   If you don’t already benefit from historical data, the best way to do so is to create comprehensive questionnaires that business leaders and key professionals fill in.

4. **Put business continuity recovery strategies in place**

   When working on recovery strategies, there are some aspects you need to consider:

   - **What are your key departments, and what would it take to enable them to perform their work?**
   - **What does it take to meet the demand for products or services in case of potential business interruptions?**
   - **Which projects/clients should be prioritized?**
   - **What departments need to be moved to a different premise (e.g., office building) if your facility or equipment is impacted, and which can work remotely?**

   By addressing all these matters, you increase your chances of developing a solid business continuity plan.

5. **Test and update**

   By constantly testing your business continuity planning and making improvements, you ensure that it is continuously updated and keeps up with your industry’s and the world’s challenges.

Wrapping Up

Business continuity and disaster recovery planning are a must for companies nowadays, enabling them to perform risk management procedures that limit downtime and restore business processes.

Still, since the topic is so complex, an organization’s ability to do all these alone might be limited, so working with your managed service provider is an excellent way to ensure your people, IT infrastructure, and data are protected.

FAQs

How do business continuity and disaster recovery work together?

Business continuity and disaster recovery plans are complementary. While business continuity is responsible for keeping operations running, sometimes to the minimum, in emergency office locations, disaster recovery focuses on restoring data access and normal business operations after a catastrophic event occurs.

Which comes first, BCP or DRP?

Disaster recovery and business continuity strategies help your business prepare for artificial or natural disasters. They are both equally important and implemented when disaster strikes. A broader business continuity plan requires restoring data access and IT functions, all elements disaster recovery covers.

What are common business continuity risks, and how do I identify them?

The list of potential issues is unique to each organization and entirely depends on the business's location, industry, size, and responsibilities. The best way to identify risk is by having management fill in questionnaires and discuss them in dedicated meetings that bring together senior leaders, subject matter experts, and external advisors.

Common business continuity risks include:

- **Data breaches**
- **Cyber attacks**
- **Terrorism**
- **Natural disasters**
- **Human errors, such as deleting a backup, opening malware, etc.**

Want to learn more about cyber threats?

Download this Threat Term Glossary and discuss the threats unique to your business with your MSP.

DOWNLOAD NOW