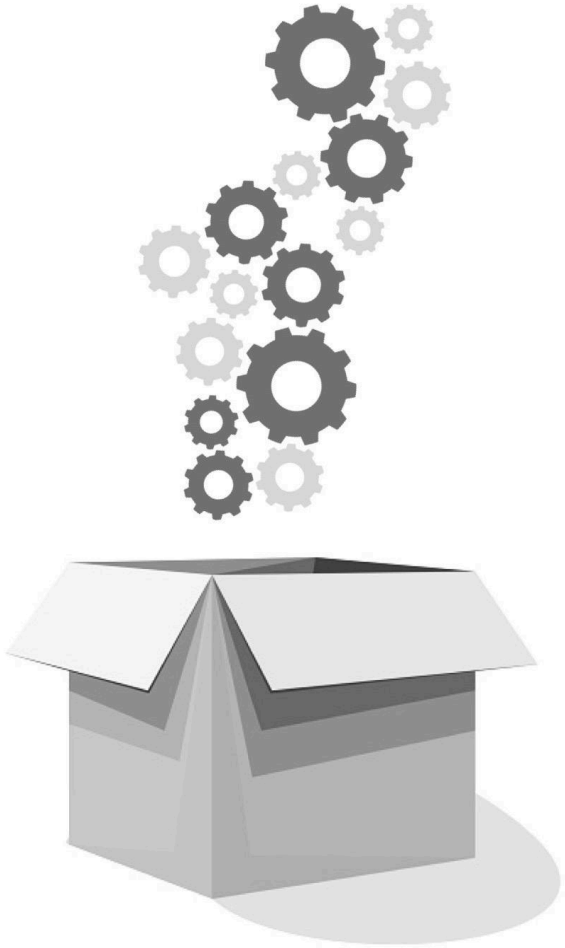
IT Disaster Recovery

A Brief Intro

Author | Paula Queiroz

Last Review | December 2023

Contents



About this Document

This document has the sole purpose of introducing the concept of IT DR (Disaster Recovery) as part of but not to be mistaken with BCP (Business Continuity Plan).

Why IT DRP isn't the same as BCP and data backups alone aren't "IT DRP" will hopefully be clarified.

We will briefly discuss why we absolutely need to have a tested, fully fit for purpose DRP.

We will also discuss why IT DR must be treated collaboratively and not thought of as a "black box-like IT-thing" only the IT team needs to be aware of.

We will finish this document with some Q&As.

Designing for Failure

Disasters happen, things get broken - matter of fact, there is no arguing against that so, when talking IT, to cater for this probability that something will fail big-time, we protect ourselves through preparedness, in the shape of what has been called "designing for failure".

Designing for failure means many things in practical terms, ranging from ensuring high availability and fault tolerance to cater for physical damage to a small hardware component in a datacenter, all the way to commissioning highly robust disaster recovery environments that allow for resuming all IT systems and services in a fast, totally automated fashion.

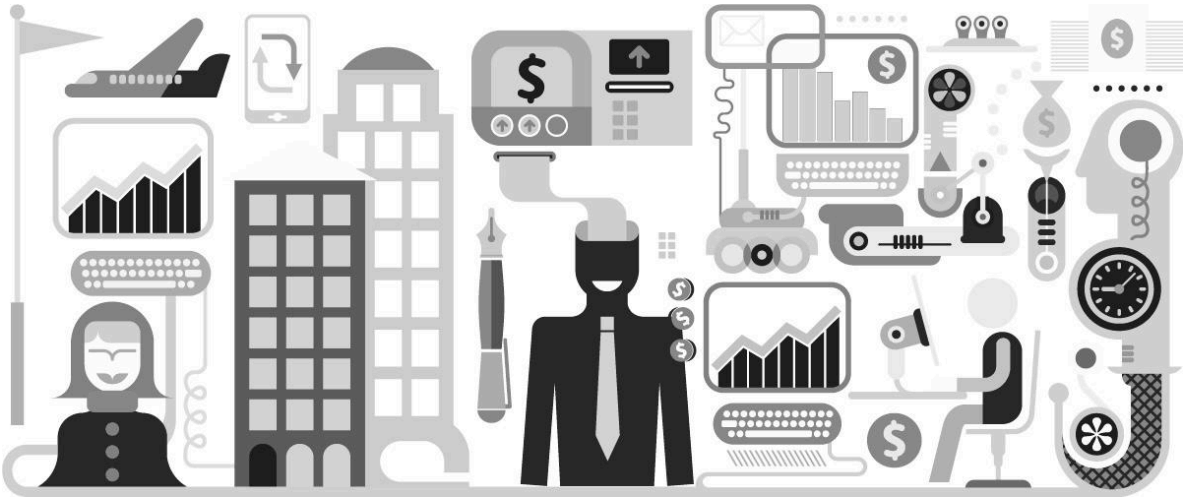
Whether we're talking redundant physical components on a server or the orchestration or a DR plan, the aim is always to withstand failure or, if the failure is not withstandable, recover from it quickly, avoiding or minimizing as much as possible any service disruption, and therefore avoiding loss of revenue and reputation.

DR and BCP

Because they are prone to being used interchangeably, even though they are different things, we will start by having a look at the differences between/definitions of DR (Disaster Recovery) and BCP (Business Continuity Plan).

Additionally, later on, we will also look at the differences between IT DR and data backups.

BCP (Business Continuity Plan)



The BCP defines how an enterprise (the whole enterprise) resumes its normal activities (business continuity) in the event of a major disaster.

To do this, at the very least, the enterprise will rely on a Business Impact Analysis, the results of which will provide the foundations for the definition of criticality and priority of business processes and services, which will be specified in the BCP.

Needless to say, the BCP's scope will be business-wide, and is by no means IT-focused. It will normally be produced by a BCP committee including senior management, and in collaboration with heads of departments.

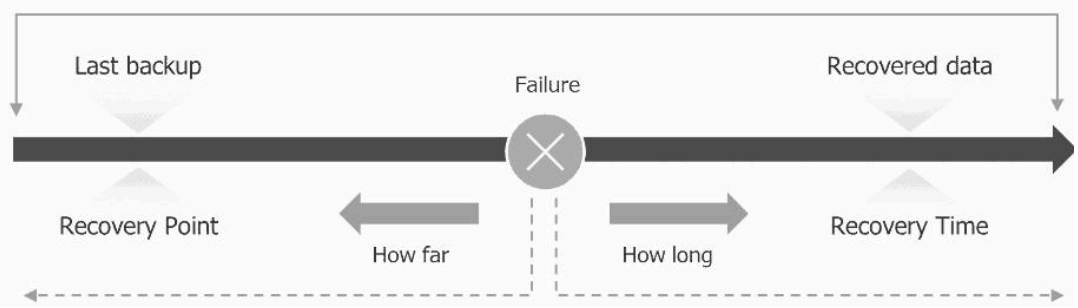
The IT Department will be involved, but will by no means be expected to produce a Business Continuity Plan!

BCP (Business Continuity Plan)

Very importantly, the BCP will also specify the amount of data of which the loss is tolerable in the event of a major disaster, and how long it is acceptable to wait before the business processes are resumed – the RPO and RTO, where:

RPO (Recovery Point Objective) defines the time from which the latest backup available to restore from must be dated.

RTO (Recovery Time Objective) defines the maximum admissible downtime, in other words, when the services are expected to be back up.



For instance, if a major disaster was to happen at 18:00, and the RPO for system/service "X" was 4h, and the RTO 4h too, the backup from which the system would be restored would have been taken at or after 14:00 (T-4h), and the system should be up and running at or before 22:00 (T+4h).

The system/service prioritization and the definition of RPOs and RTOs will often be done in agreement with or approved by business customers, so there will often be a contractual obligation to respect what's been defined on the BCP.

Failure to do so can constitute a breach of contract subject to legal action and financial losses, not to mention the impact on the business reputation and potential loss of customers and revenues.

BCP (Business Continuity Plan)

With the possibility of remote working having become standard in most organizations, the need for staff relocation to dedicated DR-PCP facilities for business continuity purposes has become less common but it, however, important to notice that, if such requirement still exists, it will be defined in the BCP also.

When it comes to IT, to be put into action, the BCP will rely on the IT DR plan, which will provide the guidance needed for making the IT infrastructure required for the business applications to run available in a timely manner.

DRP (Disaster Recovery Plan)

The DRP describes, step by step, how to recover from a major impact incident or full disruption of IT functionality, including in the event of loss (total or partial) of the primary IT infrastructure.

In this sense, the IT DRP is the process/description of the procedure for getting all the services and systems which business processes depend on (as per the BCP) running.

Disasters of many natures may trigger the need to invoke a DRP and trigger the failover to a DR site; they can be natural, structural, man-made, result from a major security breach, etc. and, in some cases, can result in rendering the facilities hosting the datacenter fully inoperational and/or inaccessible which, for the obvious reasons, is catastrophic if we're talking on-premises.

IT DRP (Disaster Recovery Plan)

Given the aforementioned, whatever the DRP, the DR site should always be at considerable distance from the primary datacenter.

In the event of, for instance, a natural disaster such as an earthquake, big flood, etc, if the DR site is next door to the primary datacenter, both are likely to be equally affected, rendering the whole DR solution useless.

The thought process is similar to when we commission cloud-based components/services across multiple availability zones or even regions.

The DRP will assume the need for IT functionality to be resumed using an infrastructure hosted elsewhere other than the primary datacenter, and will provide precise guidance on how to do it, relying on many components to do it.

One of these components will probably be data restores (file, system, etc) from backups.

Data Backups

Backups (and snapshots, which are basically also backups) are either prescheduled or manually triggered copies of data (files, applications, databases, system…) as it was at the time the backup was taken.

Backups can be done to disk, to tape, offline, via the internet or via dedicated links, they can be kept onsite or be taken offsite (for security and compliance reasons and to be used for DR purposes), and they can be full, incremental or differential.

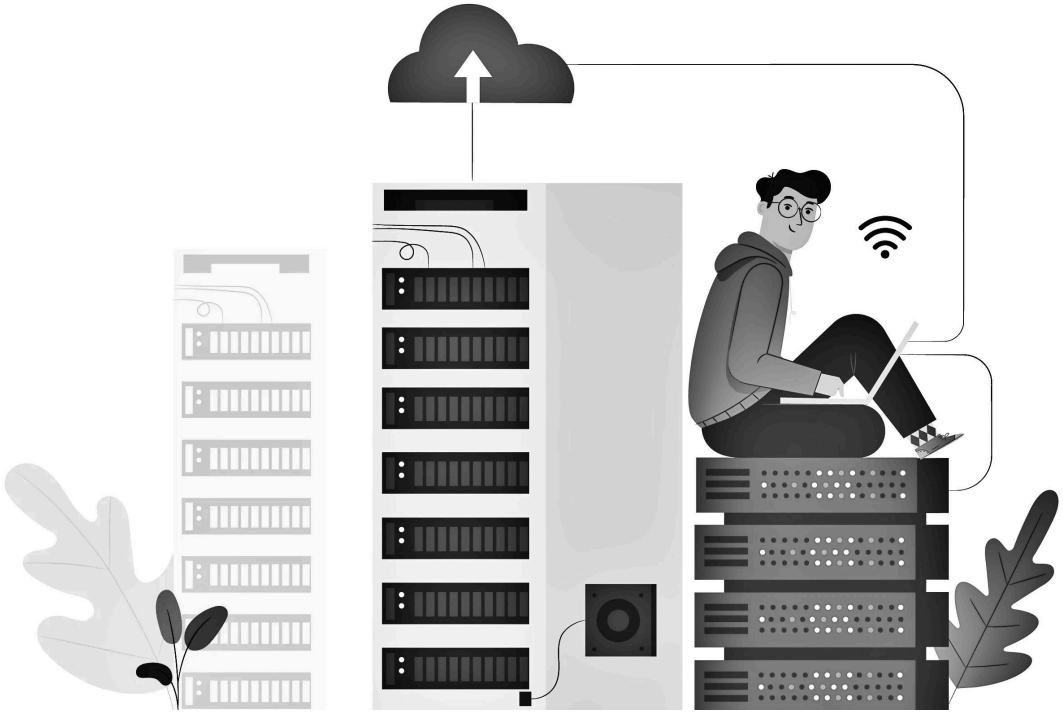
Backups are an efficient way to ensure the retrieval of lost or corrupted data through restores, and a simple restore will normally follow a manipulation error, limited data corruption or non-generalized, contained system failures.

In this sense, the practice of regularly performing backups doesn't assume that a major disaster will happen that will widely affect the IT infrastructure – backups and restores are the stuff of everyday life.

Backups are also a cheap way to ensure data (and different versions thereof) are stored for a certain amount of time for legal and compliance reasons, in case data which isn't accessed frequently can still be retrieved should the need ever arise.

Whilst data backups will likely be called upon if a DR failover is required, on its own, a backup solution cannot be considered anywhere near a DR solution.

DRaaS (DR as a Service)



Cloud-hosting (IaaS, PaaS, etc) will inherently provide most mechanisms needed for DR, given that, by default, Cloud Providers have highly resilient datacenters with assured hardware redundancy, geodistributed multisite hosting, etc.

However, for one reason or another, most businesses are still far from having 100% cloud-based datacenters, so we'll be focusing on on-premises datacenters.

Even if the datacenter is on-premises, cloud functionality can still be highly beneficial in terms of DR-BCP and can go from a "hybrid" basis where, for instance, only backups are kept in the cloud, all the way to a fully cloud-based DR solution: DRaaS (DR as a Service).

DRaaS (DR as a Service)

DRaaS can greatly simplify and speedup the process of failing over to the DR environment, as well as having the potential to make it far more cost-efficient than an on-premises DR solution:

As everything cloud-based in general, the deployment of the environment can be done much faster and is normally easier than the deployment over an environment which relies on the commissioning and configuration of physical equipment.

Albeit faster to commission, and easier to configure and manage, DRaaS offers the same functionality as a physical DR site (compute, storage, security, etc).

The lack of need for the manipulation of physical devices removes a layer of complexity and a potential source of problems and human errors from the overall solution.

The offsite storage of critical data is done by default (and that data will likely be stored across multiple devices on the cloud-provider's datacenter(s), which will be made of highly resilient hardware components).

Like everything-cloud, it will be highly and easily scalable by default.

Schemes that allow for the reduction of costs to basically "only pay when it's used" can greatly decrease the cost associated with having a robust DR solution in place.

Automation and orchestration

For the obvious reasons, the DRP should be put into motion as quickly and efficiently as possible, therefore, the more is automated, the better.

An automated DR solution has not only the benefit of allowing for services to be resumed in a faster way than if the tasks involved were to be executed manually, but it also reduces the risk of errors and failures inherent to manual, human intervention.

From in-house scripting (which is far from ideal), to fully automated out-of-the-box public and private cloud products and services, there is a lot to choose from in terms of automating tasks and orchestrating different DR scenarios, and the choice will largely depend on the business needs and financial resources available.

So, what's important to retain is that the more is automated and orchestrated, the faster and easier it will be to execute the recovery and, if properly configured, the more likely it is to work without hiccups.

DR Run Book

The DR Run Book must include everything, step by step, that is needed for the DR plan to be invoked and for a successful failover to a DR site to be executed.

A hard copy of the DR Run Book should be available and easily accessible to the IT department, of which the members should know exactly where to find it very quickly.

Needless to say, the DR Run Book should be continually updated and the updates should always be communicated to the BCP committee.

Updates should reflect the updating of risk analysis, inventories and infrastructure/services updates.

- The way the business prioritises something new will define how the IT DRP treats that “something new”.
- If something is decommissioned that is included in the IT DRP, the Run Book should be updated accordingly.

There is no point in having a DR Run Book or DRP in general if the recovery process described does not apply to the environment which is actually in place.

DR Run Book

Some of the things the DR Run Book will include are:

Definition of DR actors:

In a DR situation, the chain of command must be clearly specified. One person, not multiple people, should be coordinating the entire process, and this person on the top of the chain of command should be the one declaring the major incident and approving the triggering of the failover to the DR platform.

Roles and responsibilities of the different DR actors must also be clearly expressed. This too will be included in the Run Book. If disaster strikes, everyone involved in the IT DR process should be prepared and know exactly what they're expected to do well in advance.

Some of the fundamental actors every DRP should name and define the responsibilities of are the DR-BCP manager/coordinator (top of the chain of command), technical staff of different relevant expertise (SMEs, Subject Matter Experts), a communications manager (because it's a bad idea to expect clear communication in a crisis when there's no single, dedicated point of contact), and heads of department.

Even though the Run Book should be granular and explicit to the point that anyone with the right level of access should be able to execute all the steps needed for a successful failover, every DR actor should have a deputy with the same level of knowledge concerning what they're supposed to do and how to do it if the former is unavailable during the crisis time. This will help avoiding panic by alleviating the stress of having to learn how to handle the crisis during the crisis itself.

DR Run Book

The Communications' Plan:

During a disaster or any major IT outage causing disruption to the services meaningful business processes rely on, clear, frequent communication is crucial both internally and externally.

A communications plan is also an important part of the Run Book, and it should include templates for the communications to be sent out depending on the type of scenario, as well as its intended audience (internal and external, such as customers, suppliers, etc).

In a moment of stress where many things (many of them being bad) are happening simultaneously, writing ad-hoc emails to clients and partners who won't be happy already is not the best idea. These templates will help up maintain an image of professionalism and being in control of the crisis.

From experience, communication with stakeholders and customers is one of the most important and challenging parts of ensuring a peaceful switchover to DR, as efficient communication will result in less stress, and more focus on the job at hand.

Staff Engagement

Even though those who are directly involved with either the definition or the execution of a DR-BCP are expected to be the ones holding the deepest level of knowledge concerning the whole process, it is important that all the staff who a major incident will have an impact on are aware that such plans exist and have an idea what they're about.

Basically every single employee will be affected in no matter how small a way, so everyone working for the business should receive some sort of training concerning the DR-BCP and no one should find out that such thing is exists during the disaster itself.

Periodic awareness campaigns are highly recommended. The IT DRP reflects the business needs and, in the event of a disaster, the business needs can only be met through efficient IT DR, so cooperation and two-way communication will be necessary not only to create but also to maintain the IT DRP.

Testing the IT DRP

The importance of thorough testing of the IT DRP cannot be stressed enough!

Regular testing must be done in order to ensure that the solution in place is fit for purpose as realistically as possible: if issues are to be found, they best be found in a controlled environment where the failback to the primary site can be done at any moment.

If the IT DR(-BC) plan is only "tested" when a real major outage occurs, we might have the unpleasant surprise of being unable to perform a failover, which would mean having to wait until the initial issue is resolved before resuming service, which may not meet our RTOs and, as mentioned before put is in a situation of contractual breach.

Keep it in mind, however, that performing a serious, truly validating IT DR test is not easy. It takes a lot of planning and, again, a lot of collaboration between IT and the business. Business apps and process are likely to experience some sort of disruption, and part is the tess will, as mentioned, consist of having users doing their normal tasks

Starting services and applications in the DR site, or verifying that backups can be restored do not qualify as testing the DR. A thorough test involves having the business process running in production-mode from the DR site. Only when this is successfully done can the IT DRP be said to be tested and proven to be fit for purpose.

Any Questions?