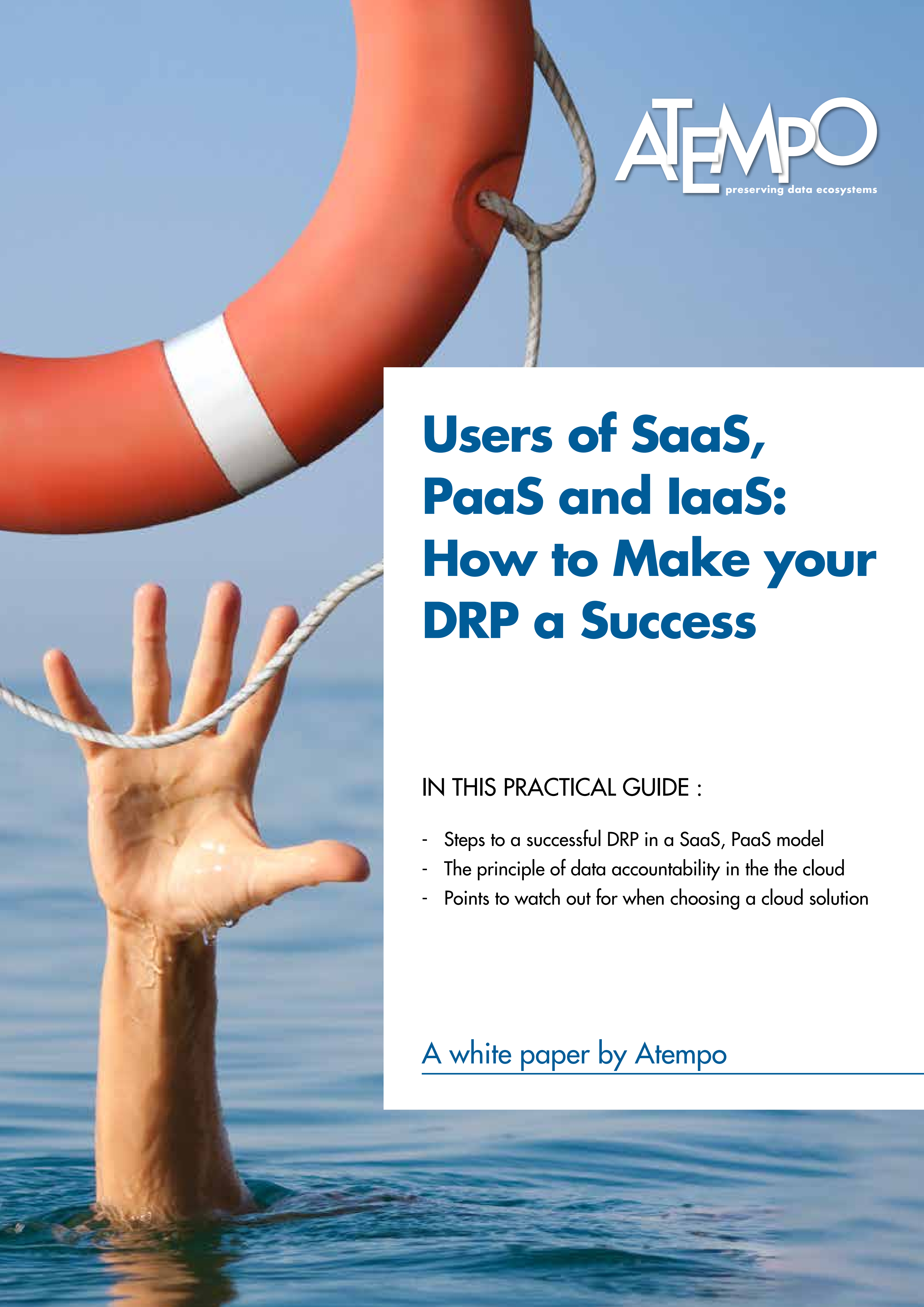


ATEMPO
preserving data ecosystems

Users of SaaS, PaaS and IaaS: How to Make your DRP a Success

IN THIS PRACTICAL GUIDE :

- Steps to a successful DRP in a SaaS, PaaS model
- The principle of data accountability in the the cloud
- Points to watch out for when choosing a cloud solution

A white paper by Atempo

Table of content

Executive Summary

With its flexibility, its simplicity, its storage capacity and its cost savings, the majority of companies today consider cloud technology to be a positive for their organization. In the early 2010s, businesses massively adopted cloud computing. Convinced by the capacity, feature sets and future promise, many have mis-evaluated **the scope of delegation entrusted to their service provider**, either through over-confidence or a lack of vigilance. In other words, by entrusting the cloud provider with their most valuable assets: data, they have put this very data at risk.

Cloud service providers offer several safeguards to protect data and applications from cybersecurity threats or hardware failures. But, like anywhere else, human errors or malware threats can lead to data breaches. An increasing number of companies have identified security incidents in the cloud. And despite talking up their resilience, the fact remains that cloud providers are not immune to disasters. This point is essential: **companies remain 100% responsible for their own data**, regardless of the infrastructure chosen to store this data: local, hybrid or cloud. But how do we protect our data when using a cloud service provider? How can we implement a DRP (Disaster Recovery Plan) to restarts activity when disaster strikes? How do we keep control of our data, even if this data is in the cloud? What level of vigilance is required when choosing a cloud service provider?

This white paper provides recommendations on **the best strategy to follow and how to maintain business continuity when implementing a delegation of service in the cloud.**

Chapter 1: Background

The digitization and increase of online activities have led to an explosion in the amount of generated data generated. According to the international research firm, IDC, **the global volume of data will be multiplied by 3.7 between 2020 and 2025. It will then be multiplied by 3.5 every five years until 2035 to reach 2,142 zettabytes.** The covid-19 pandemic and the democratization of home office working have accelerated this phenomenon by disrupting the way we work and generate data. And that's not all: the arrival of 5G and the development of IoT technology will substantially add to the volumes of data produced.

Fast-growing data flows are causing serious difficulties for companies' IT infrastructures. Firstly, they contribute to the problem of data silos. As the amount of data produced increases, data is divided between the different departments in a company. These entities rarely communicate with each other, and each considers itself the owner of its data. Yet data is now a strategic asset across all industries and allows us to make better decisions and gain competitive advantages. Organizations have an important and complex challenge to face : breaking down data silos in order to make better decisions and improve the performance.

The other big challenge for companies is **the storage of these significant data volumes.** Cloud computing has allowed them to increase their storage capacity while reducing costs and on-prem physical storage space. With the rise of remote work, the cloud offers employees access to data, regardless of their location and the device used (computer, tablet, etc.). The cloud enables collaborative work by allowing several people to access the same document at the same time. Unfortunately, many business leaders have a misleading perception of cloud technology and believe that everything is managed by the service provider. The reality is often quite different.

Remember that the **cloud is not infallible** and data may be exposed to risk. According to the Global Data Protection Index conducted by Dell in 2019, one in three business worldwide has experienced irreversible data loss. The news regularly reminds us that a disaster causing the loss of critical data can threaten a company's existence : financial consequences, reputational risk, downtime, etc.

To remember

One in three business worldwide has experienced irreversible data loss !

Several major disasters in recent headlines have shown the limits of cloud services: the data center of a major French hosting company destroyed by fire, an island ravaged by a hurricane causing the loss of a biotechnology company's data, severe breakdowns affecting services of a major storage company, etc.

These events, impossible to predict and with devastating consequences, have been named "black swans" by the Lebanese-American statistician Nassim Nicholas Taleb. But whether it is small incidents or significant disasters, the risk of data loss should always be factored in.

In addition to these risks, organizations have to fight against cyber-crime. The number of ransomware attacks against companies, cities or hospitals, increased by 151% in the first six months of 2020 according to a survey conducted by the American firm Neustar.

These attacks cause the loss of valuable data when the ransom is not paid. Even backups that ensure data is available when other protections have failed are now the target of ransomware. Cyberattacks are no longer categorized as «black swans» because of their increased probability. It becomes critical not only to protect the production tool and data, but above all to have a plan to retrieve the activity after an incident.

Unfortunately, many companies, and especially small structures, do not have a clear view of who is actually liable.

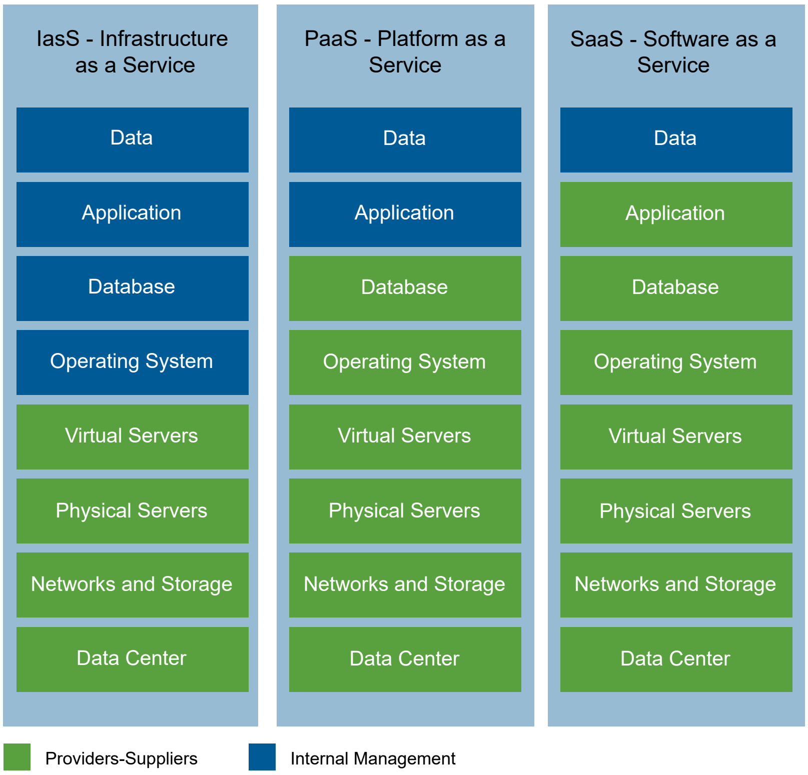
They often consider that their service provider is responsible for their data ecosystem. However, the responsibility of each party is mentioned in the contracts established between companies and their cloud solution provider.

To remember

Whatever form of delegation a company chooses, Saas, PaaS or IaaS, data's protection is always under its responsibility.

The notion of shared responsibility is a key element of the "as a Service" model. This model helps determine the role of the service provider in managing servers, applications and databases. However, there is one constant: **whatever form of delegation a company chooses, data's protection is always under its responsibility.**

The following figure illustrates **the shared responsibility model** and shows that **regardless of the type of delegation (SaaS, PaaS or IaaS), data security is always under a company's responsibility:**



IasS - Infrastructure as a Service	PaaS - Platform as a Service	SaaS - Software as a Service
🟦 Data	🟦 Data	🟦 Data
🟦 Application	🟦 Application	🟩 Application
🟦 Database	🟩 Database	🟩 Database
🟦 Operating System	🟩 Operating System	🟩 Operating System
🟩 Virtual Servers	🟩 Virtual Servers	🟩 Virtual Servers
🟩 Physical Servers	🟩 Physical Servers	🟩 Physical Servers
🟩 Networks and Storage	🟩 Networks and Storage	🟩 Networks and Storage
🟩 Data Center	🟩 Data Center	🟩 Data Center

🟩 Providers-Suppliers 🟦 Internal Management

Illustration: The principle of shared responsibility in the IaaS, PaaS and SaaS models

In 2018, consulting firm Gartner predicted that **by 2022, at least 95% of security incidents in the cloud will be attributable to customers.**

This data confirms that the service providers are rarely responsible for the security of their customers' data and shows the importance for businesses to understand that in the cloud, anything can happen.

The dependency of the companies on their IT services highlights the need to protect their data through the implementation of best practices, before being faced with an unplanned incident. These are not only intended to protect data, but to restart the activity as soon as possible after the disaster.

The implementation of a DRP (Disaster Recovery Plan) is an integral part of these best practices, regardless of the size of the business. This plan is about managing risks and regaining access to a functional IT infrastructure after the disaster.

The DRP should not be confused with the BCP (Business Continuity Plan) which outlines procedures to implement to maintain essential business activities. The BCP is a short-term solution to rapidly respond to a critical situation.

We estimate that 40% of companies that have suffered from a major incident causing the destruction of their IT infrastructure and the loss of their data will disappear if the downtime has exceeded 72 hours.

It is therefore essential to implement a DRP and regularly test it in real-life situations. Bear in mind the key point data security is under a company's responsibility. On the strength of this, organizations will know how to protect their most valuable and strategic assets: data.

To remember

40% of companies that have suffered from a downtime exceeding 72 hours will disappear

Chapter 2: Assess the Risks and Prepare the Steps for a Successful DRP

In January 2009, a US Airways Airbus 320 lost power in both engines after hitting a flock of birds after taking off from La Guardia airport in New York. The flight crew made what they felt to be the only viable choice: ditch the plane in the Hudson River east of Manhattan. The pilot Chesley Sullenberger and copilot Jeffrey Skiles remained exceptionally calm throughout. They even took out, read and followed the emergency procedure documentation to ensure they were approaching the water at the right speed and inclination. The pilots' decisions and subsequent heroic execution of the Hudson water landing were perfect examples of technical experience, instinctive calculations and **specific procedure**.

Because emergencies are by nature rare and stressful moments, we need a clear set of processes to avert or attenuate the impact of disaster. Even on terra firma, things can go seriously wrong.

Take the example of the total or even partial loss of a company IT infrastructure. IT may not put lives at risk, but the survival of the organization is indisputably at stake. When IT teams reach for their Disaster Recovery Plan documentation, they need to be sure that predefined action buttons they press will be the right ones to get systems and data back where they belong with as little lost business as possible.

One stone-cast certitude is that **any attempt to restart IT systems without following tried and tested emergency recovery procedures will doom the company to extended or even permanent blackout.** And time is very much money in this case…. So, what's in a DRP? The short answer? A lot.

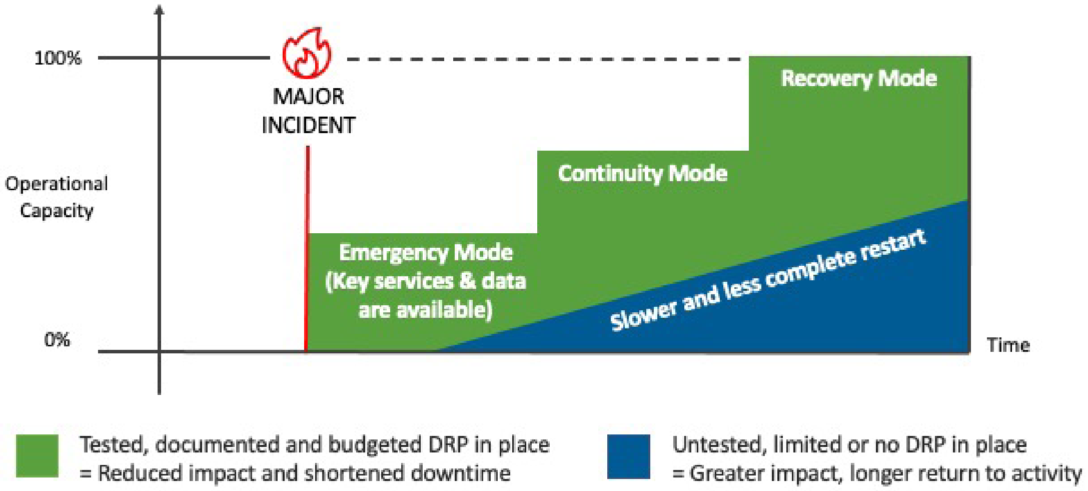


Illustration: Impact of the DRP test on the return to operational capacity and recovery time

A fully-fledged DRP document will **detail what machines, applications and data need to brought back up and in what order.** It will run to tens or even hundreds of pages and include hardware and software recovery procedures. Is the server room still in working order.

Is their power? Network availability? Who will check and perform each recovery procedure, in which order etc. etc.? **Each procedure will be fully and regularly tested in real or near-real conditions.**

Because we live in hybrid world where our systems and data are rarely in one single location, the restart plan will call on different resources that may be more or less impacted. If a data center fire removes access to a web server, we will need to know where the latest offsite backup is located and how to restore it to another web server and how to reconfigure the DNS to provide site access to your customers and stakeholders.

Standard procedure recommends at least 80kms between two data center storages to reduce to near zero a massive regional outage following a major natural disaster for example.

No single company nor any SaaS provider are exempt from a disaster, and you are obliged to ask yourself what would happen if your cloud CRM service lost data through a cyberattack for example.

How quickly can you restore data from an off-site backup to retrieve crucial and sensitive customer information? If your IaaS provider loses a data center, will you be able access a failover server or fall back to an on-prem infrastructure within an acceptable time frame?

Each data set or business process must be attributed a risk factor. For example, on a scale of 0-10 how serious would be the impact of losing data? What are the acceptable RPO* and RTO* for each department, data set and application?

- RPO is the quantity of acceptable data loss or service downtime in the event of a serious incident.

- RTO is the acceptable length of time to be without a service, application or data until normal service is resumed.

Your organization may accept only a few seconds' loss of access to a banking app, a few hours for a mail server or even a week or more for Human Resource archives. Because the costs of storing multiple backup copies is tightly linked to cost, it is rarely possible to have RPO / RTO close to zero (zero data loss and zero time before restart).

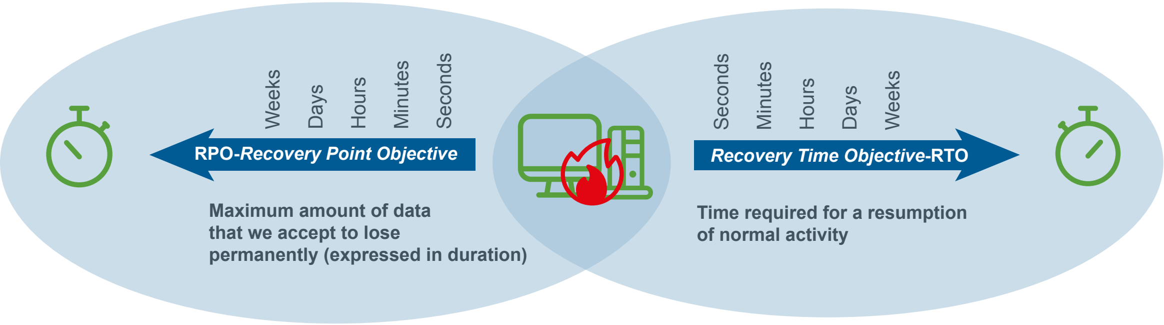

Weeks
Days
Hours
Minutes
Seconds
RPO-Recovery Point Objective
Maximum amount of data that we accept to lose permanently (expressed in duration)
Seconds
Minutes
Hours
Days
Weeks
Recovery Time Objective-RTO
Time required for a resumption of normal activity

Illustration: RPO or RTO, the difference

The less data you accept to lose and the shorter the time to recovery, the higher the cost.

Choices need to be made including a detailed cost assessment that underpins each DRP. How much will each service or departmental downtime cost a business in the event of a serious incident?

As mentioned in the first section, the responsibility for data lies with the owner of this data. As any lawyer will tell you, "The devil is in the small print." **Read your contracts and go over your internal and external SLAs** (Service Level Agreements) and, if necessary, renegotiate to tailor them to your overall needs. Risk assessment and DRP procedures are also integral to many internationally recognized norms including ISO 2700.

But even by following norms and stacking insurance policies, you are the guarantor of your customer's, patients or employees' data, whether you are a business leader or a CIO. Make sure to have a documented and tested DRP. As a final checklist and to summarize the steps on accessing and rebuilding internal and external applications and systems (on-prem, Cloud, IaaS, SaaS etc.):

- **Understand and identify the potential** impacts case-by-case,
- **Perform a data loss risk** assessment,
- **Identify acceptable RPOs / RTOs** for each department/application,
- **Evaluate the cost vs criticality of your data and applications,** (backup repository on Worm type technologies …),
- **Test regularly the entire DRP**, including with your service providers,
- Ensure that your service providers are in activity and remain viable,
- Etc…

To remember

The 3 keys to a successful DRP:

1. Regular testing of the existing DRP
2. A study of the risks
3. An evolution of procedures, if necessary

Risk assessment, procedure documentation and DRP testing are time consuming and costly. The entire process exceeds the scope of a single manager or even a complete IT team. Management and DPOs will be key stakeholders in what is an ever-moving scenario. Help is at hand and you can call on:

- **Dedicated consulting firms** who can interview stakeholders and assist in drawing up and implementing a partial or total DRP.
- **Technology partners and integrators** can ensure new software and hardware resources are available.
- **Data protection and recovery solutions** are the cornerstone of any DRP. Choose wisely and test partial and full restores regularly.

These points basically comprise your organization's get-out-of-jail card that protects you in a situation you hope will never arise!

Chapter 3: Subscribing to Cloud Services: DRP Recommendations

Regardless of the type of delegation chosen, SaaS, IaaS, or PaaS, companies are the decision makers when building their DRP. There are **8 key points to consider** when implementing **a delegation with a cloud service provider:**

READ CONTRACTS CAREFULLY

The first reflex is to have all the operational delegation contracts reviewed by your legal department. Keep in mind that going to court in the United States could be very expensive. However, reading contracts is not just for your legal teams. Certain points should be carefully studied by the IT department, in particular the level and scope of the service.

Contrary to popular belief, a cloud service does not automatically ensure high availability of your applications or automatic replication of your data, or even the externalization of your backups or automatic backup of your data. Remain vigilant and read the contracts established with each service provider. Pay particular attention to:

1. The scope of the service: Are we looking to guarantee access to a physical machine? To a virtual machine? To an application? What is the exact number of users etc.?

2. The service-level agreement (SLA) for the applications. If the clause is missing, we highly recommend you to add them so as to define the service quality levels to provide, especially the availability and unavailability rate guaranteed by the service provider.

Keep in mind that an availability of 99% represents a possible downtime of 7.2 hours per month. The table below provides a grid for these metrics by converting them into annual or monthly downtime.

Specify the time slots for these availabilities (365 days and 24 hours for instance) and the authorized maintenance periods.

Try to think about the penalties for the service rate clauses to be respected. If the service availability rate is important to your business, ask your service provider to respect it. In the absence of a penalty clause, you are free to add one and amend it to obtain financial compensation and / or pass on financial repercussions to your service provider;

To remember

Have your legal department carefully review your contracts

RATE	DOWNTIME PER YEAR	DOWNTIME PER MONTH
99%	87 hours or a total of 3.5 days	7,2 h
99,9%	8 hours, 45 minutes, 36 seconds	43,2 min
99,99%	52 minutes, 33.6 seconds	4,32 min
99,999%	5 minutes, 15.36 seconds	25,9 s
99,9999%	31.68 seconds	2,5 s

3. The commitments made regarding your data protection. Here are some interesting examples of wording that can help avoid surprises: “in case of force majeure, the contract will end after one month”, “the client is responsible for their own backups” or “the client is responsible for the externalization of their backups”.

Consider validating your delegation contracts by a lawyer. He will have an additional take beyond the “IT reading” and automatically control the jurisdiction. The referral to the Court of Justice of the United States can be very expensive. You can proceed in the same way with your insurer, it is always better to get his opinion before a disaster.

DATA PROTECTION

It is very important to understand that a replication is not a backup of your data and does not protect your business from data loss and malware.

4. Data replication consists of either ensuring access to applications and data or making several copies of business data available on different storages to share access to the data from multiple sites, without interfering with the others. Some replications can be done in real time (synchronous replication), others at regular intervals (asynchronous replications).

Data replications involve a copy of the data, but bear in mind that they only capture an up-to-date version and fail to rebuild an historic.

On the contrary, backup captures data in regular time intervals and in the long run. It allows you to go back in time over a predefined period and restore data as it was at a given time, individually or within a coherent whole. Backup is the basic tool of any disaster recovery plan.

5. The cloud provider’s offer that you are considering probably describes a system dedicated to your data security without even mentioning the word “backup”. We encourage you to be curious. Any compromise will have consequences on your data or business sustainability.

THE 3-2-1-1 BACKUP STRATEGY

The rule is simple : you should have 3 copies of your data on two different media with one copy off-site and one copy offline. To store a copy offline, you need to apply the “air gap” backup rule, either by moving a copy so that it is isolated and externalized (removable disk or tapes) or by “functional” isolation (servers stopped so that network access is not active). The “Air Gap” backup guarantees that the copy is not altered or deleted.

The retention periods of your backups must be long. You should never shorten retentions, even if this incurs costs. If storage costs are an issue, choose a backup solution that has at least deduplication of “at rest” backups, that is, on the storage specific to the backup solution.

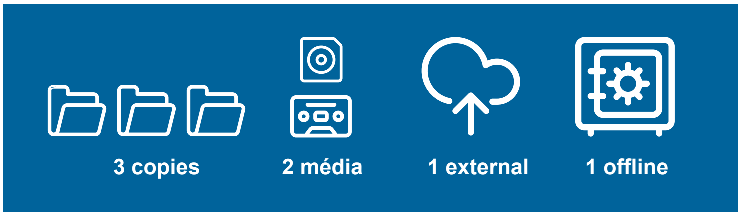


Illustration: Good practices: Backup 3-2-1

The principle is to «de-duplicate» the storage while rebuilding information on demand. Try to keep in mind that deduplication will be more effective than a compression system used alone. Ideally, try to combine deduplication and compression.

Test the benefits in terms of storage volume and remember to take into account the «time» impact of stacking these two layers of treatment, which can significantly slow down treatments.

You should also consider compliance with the laws and regulations to which your organization is subject, especially :

6. The obligations imposed on business leaders related to the implementation of procedures for securing information systems. Please notice that criminal liability may be incurred if a problem occurs with business data.

7. The GDPR (General Data Protection Regulation). With this regulation, the European Union is regulating the storage conditions of its nationals’ personal data. By subscribing to a SaaS offer that seems to be operated in Europe but is actually provided by a company not subjected to European laws, a company is exposed to a breach.

The penalties for not complying with the GDPR are between 2% and 4% of a company’s annual revenue.

Consider asking a DPO (Data Protection Officer) for guidance to validate your delegations and your compliance with GDPR. To avoid disappointment, we suggest that you choose a service provider subject to European laws with data located in a European country.

8. If necessary, take a few steps back and reconsider your choices made from a geopolitical and economic point of view (technological sovereignty) according to your commitment or your activity.

Conclusion

Disasters are inherent to each business and the cloud is just a fallible technology made of several machines that offer a service. Protecting your data, your most valuable asset, requires a solid understanding of the scope of the delegation entrusted to your service provider. Whether you choose a SaaS, PaaS or IaaS service offering, you are always the guarantor of your data protection.

Another big challenge for your business is about anticipating potential risks and continuing to operate after a major disaster. The preparation of a DRP must be as complete and as accurate as possible, describing the procedures to apply to restore your activity and mitigate the consequences of an incident.

Obviously, this plan must be tested as often as possible, in real-life conditions and adjusted as required. But there are other best practices such as a careful reading of your delegation contracts, regular data backups and the choice of a service provider if your business is European, subject to European laws. In this context and in order to respond to these challenges, it has become both essential and urgent to choose an European partner with expertise in data protection and disaster recovery.

About Atempo

Atempo is a leading independent European-based software vendor with an established global presence providing solutions to protect, store, move and recover all mission-critical data sets for thousands of companies worldwide. With over 25 years' experience in data protection, Atempo offers a complete range of proven solutions for physical and virtual servers' backup, workstations, and migration between different storages of very large data volumes. **Atempo**'s three flagship solutions, **Lina, Miria and Tina** are labeled «As used by **French Armed Forces**» and «**France Cybersecurity**». Selected to join the Alumni French Tech 120, a government program designed to nurture 25 unicorns by 2025, Atempo is headquartered in Paris and is present in Europe, the US and Asia with a partner network in excess of 100 partners, integrators, and managed service providers.

For more information: www.atempo.com