HOW TO PROTECT YOUR DATA AND IT

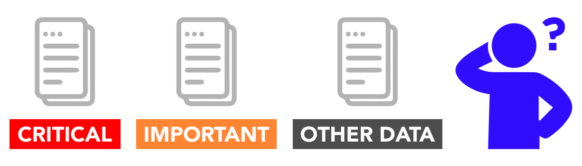
THE 8 THINGS YOU NEED TO GET RIGHT

Your guide to finding the right provider or solution for central data management services such as backup, replication, archiving and recovery.

Data is a valuable asset that is central to business performance and success, and how you use data is instrumental in facilitating digital transformation. To put it plainly, the availability and recoverability of your critical data is not a 'tick box' exercise, your choice of data management across backup, replication, archive and storage, is one of the most important decisions you will have to take.

The following list of considerations is a great starting point to getting it right:

1 Understanding the value of your data



Questions to determine ineffective and costly data management:

1. Are you storing all your file data on expensive primary storage?

This causes poor performance of your primary, tier 1 storage.

2. Are you backing up all your file data in the same way?

This creates a longer backup window than you really need and jeopardises your ability to meet recovery time objectives (RTOs).

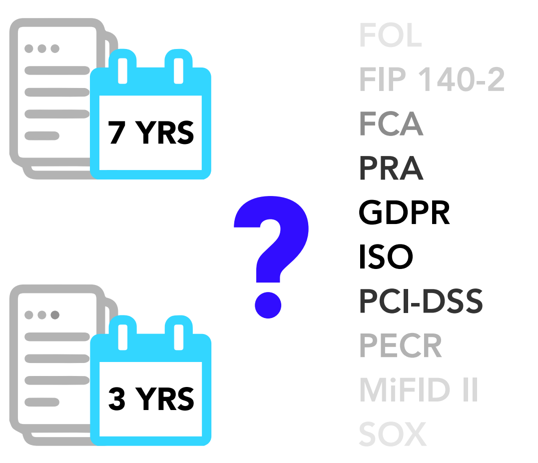
Protect all your data appropriately depending on its use and value to the business.

As a general rule:

Only **20%** of file data is business-critical

80% of file data is 'inactive' but cannot be deleted for practical, legal and compliance reasons

Only **2%** will need to be touched again, but as nobody knows which **2%**, it all needs to be accessible and indexed



2 Compliance

Make sure you meet current data protection obligations in terms of compliance with the General Data Protection Regulation (GDPR) and any industry regulations that apply to your sector.

Do you retain only relevant data for an extended time?

What assurances do you have that your provider has adequate security protocols in place?

Do you have granular control of data deletion? (from backup sets for example)

TOP TIP

Top tip from Mark Wilson, Business Continuity Solutions Architect:

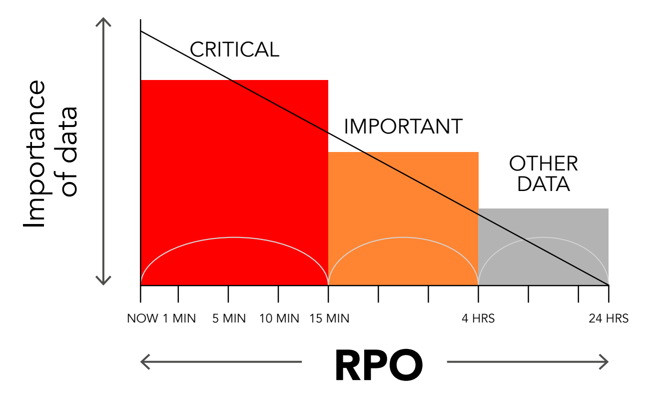
"Don't let a third-party provider or a particular solution limit or dictate your data retention policies. A third-party is not in a position to stipulate or even recommend what your policy should be. It will depend on your risk exposure, your risk aversion and the output from your business impact analysis (BIA). It needs to be aligned to your specific business requirements and include considerations around compliance with general and industry-specific legislation, the needs of your customers (or even by a specific customer), as well as your internal procedures, legal and financial obligations, and so on.

With so many contributing factors, there is no 'one rule fits all', but there are common approaches. For example, many of our customers adopt a grandfather, father, son policy – so it cycles three or more generations of data, such as weekly, monthly, yearly, or including other time frames such as hourly, daily, quarterly. This is fairly typical but by no means definitive – other customers keep all data indefinitely, which can be costly to maintain and risky to recover."

3 Recovery point objective (RPO)

How much transactional data can your business afford to lose in the event of an outage? From the last transaction, the last week or anywhere in between? Does your current solution let you choose a suitable recovery point to go back to?

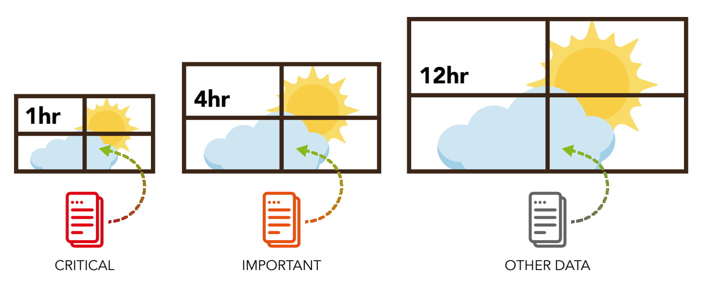
Do you have the ability to perform full or partial failovers if required? Does your solution provide the ability to failback with minimal disruption to live services?



TOP TIP

Top tip from David Davies, Business Continuity and IT Service Continuity Consultant:

"During a business impact analysis (BIA) ask yourself: "Could you recreate or accept the loss of all the work you did yesterday if the data was lost?" (e.g. that would be a 24 hour RPO if you could). Remember that the location of backups is important – sometimes there's a local backup in the same server room that would also go up in smoke in a disaster, and a remote backup to another server room which may be more out of date. Sometimes there's no remote backup, but this may be less of an issue with the adoption of cloud disaster recovery – provided you have those third-party checks in place."



4 Recovery time objective (RTO)

Does your current solution provide the ability to reinstate services by criticality, within timescales defined by your business? Where and when do you need data to be recovered to? It might depend on the nature of your outage – is your provider able to be flexible?

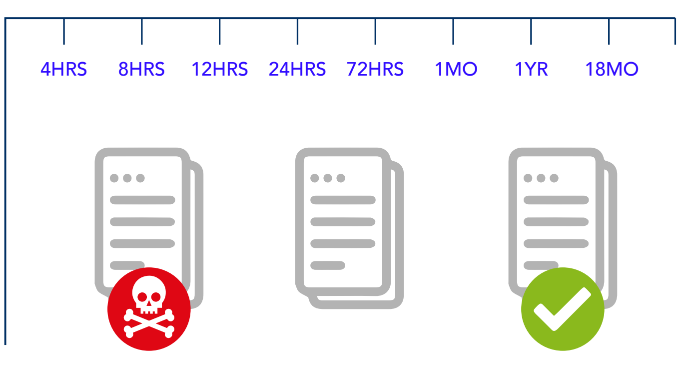
TOP TIP

Top tip from Mark Wilson, Business Continuity Solutions Architect:

"The business will no doubt want everything straight away in a serious IT outage, so having a clear RTO agreed with the business is important to fall back on. It's also important to understand your RTO in terms of the recovery order. Keeping to a plan of IT services to recover in order of importance brings order to the chaos (and perhaps panic) of IT service recovery."

5 Cyber safety

Does your solution provide the ability to roll back to before any corruption or malware attack? Does your solution have any methods of preventing the replication of corruption in recovery?



53% organisations rate security as their top IT challenge and **74%** said that their customers are now more, or much more, concerned about cybersecurity and data protection.

Larato UK COVID-19 mid-market/enterprise research

Cybercrime is now the **second highest** reason for business continuity invocations, after hardware/comms failure.

Daisy invocation statistics 2022

Are you aligned to best practice for IT Service Continuity Management (ISO 27301)? Or Business Continuity Management (ISO 22301)?

IT Disaster Recovery Plan (ITDR) or IT Service Continuity Plan: This is an IT Management level plan focussing on the decision making processes of identifying an IT disaster or serious IT outage, taking action to notify the business, restore IT services and keep communicating and making informed decisions.

Technical Recovery Plan: This provides the technical detail of how to recover IT services, including system commands and screen shots. It becomes an invaluable "go to" guide in a recovery scenario.

IT Major Incident Plan: This covers how to manage a major incident so that DR is not needed, but including how to escalate to trigger a DR invocation decision invoke DR if it becomes necessary during a major incident. At this point, the IT Major Incident Plan and the ITDR Plan may run concurrently as energy and resources are still required to fix the cause of the original incident.

Information Security or Cyber Incident Plan (with dotted lines to the ITDR Plan): Due to the unique characteristics of a cyber incident, many organisations write specific 'Major Incident' plans to react specifically to cyber incidents, generally owned by the Information Security Manager.

6 Documentation

Do you regularly update your business continuity plans and documentation? And do you get visibility or insight into the technical recovery plans of your third party providers? Especially if your data is in the cloud – where is the recovery to? What is the process? What can you expect your provider to do when an incident occurs?

Does your current solution provide assurances of development and support in line with your business applications and operating system updates?

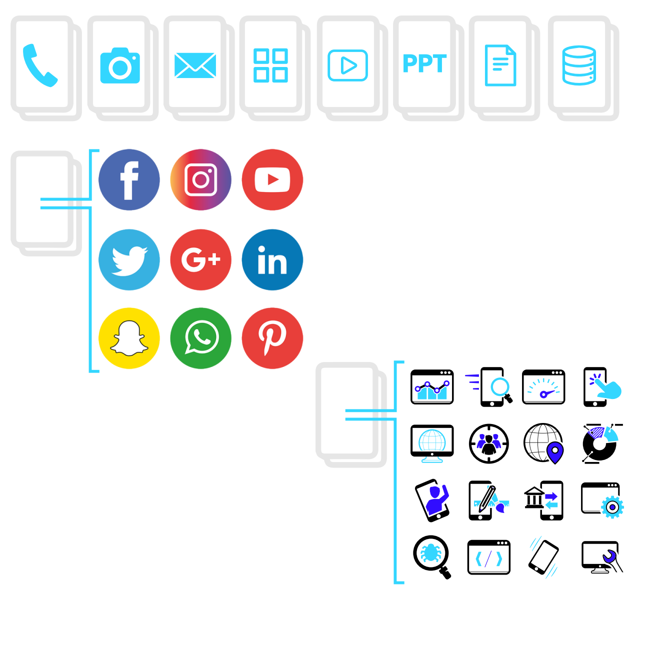
7 Testing and validation

It is crucial to have the ability to test your recovery and check if it works. An untested solution may prove to be as ineffective in a recovery situation as having no solution at all, and if you wait for an incident to happen before you find out, it will be too late.

TOP TIP

Top tip from David Davies, Business Continuity and IT Service Continuity Consultant:

"If time and resources are tight, any level of testing is better than nothing. It's a bit like turning a key in the ignition to see if it works! I must have been involved in over 100 ITDR tests and can't think of a single one that didn't have findings for improvement, and serious hidden dangers to IT service recovery can be uncovered."



8 Data growth

Data growth is creating new challenges and risks for resilience and for continuity.

- Managing data effectively is essential in order to keep control of data storage and backup costs and enable you to optimise performance of your tier one storage.
- Classifying your data correctly and applying appropriate levels of backup means you can avoid increasing backup windows that impede recovery and your ability to meet RTOs.

Data growth means spiralling costs, the need for multiple skill-sets with the knowledge and expertise to recover across all your technology/cloud platforms, and the need to provide for scalability within your third-party solutions.

By 2025, worldwide data will grow **61%** to **175 Zettabytes** with as much residing in the cloud as in data centres, 1 Zettabyte is the number 1 with 21 zeros behind it! To put that into real perspective, 1 Zettabyte is equivalent to 1 trillion Gigabytes!

International Data Corporation

In 2020 it is estimated that there will be 1.7Mb of data created **EVERY SECOND** for **EVERY PERSON ON EARTH!**

Irfan Ahmed, Social Media Today

Summary

You've got your data - now what? (resilience)	You need to be always on. IT incidents can impact business quickly. Keeping data available to your users and customers is a priority.
Getting it right can: Optimise business productivity and system performance during business as usual Allow the organisation to scale with peaks and troughs	**Getting it wrong can:** Hamper productivity and impede system performance during business as usual (BAU) Put you at risk of data loss, reputational/brand damage and lost revenue
You haven't got your data - now what? (business continuity)	**You need to recover your critical data in line with your RPOs and RTOs to minimise the impact on your users, your customers, your reputation and your bottom line.**
Getting it right can: Enable you to recover your systems and data within the acceptable RPO and RTO defined by the business Minimise the impact of any incident on users, customers and revenues	**Getting it wrong can:** Cause a protracted recovery that negatively impacts the business Cause data loss, reputational/brand damage and lost revenue

Daisy has more than 30 years' success in recovering organisations and delivering award-winning business continuity and resilience services to the UK. Our solutions give you peace of mind, increase your efficiency and help you succeed with strategic and operational goals.

Daisy can help you with all your data requirements. Our Data Protection and Recovery portfolio includes data backup, replication, archiving and recovery solutions so that you can meet every RPO and RTO your organisation demands.

We're here to talk:
enquiries@daisyuk.tech
0344 863 3000

daisyuk.tech