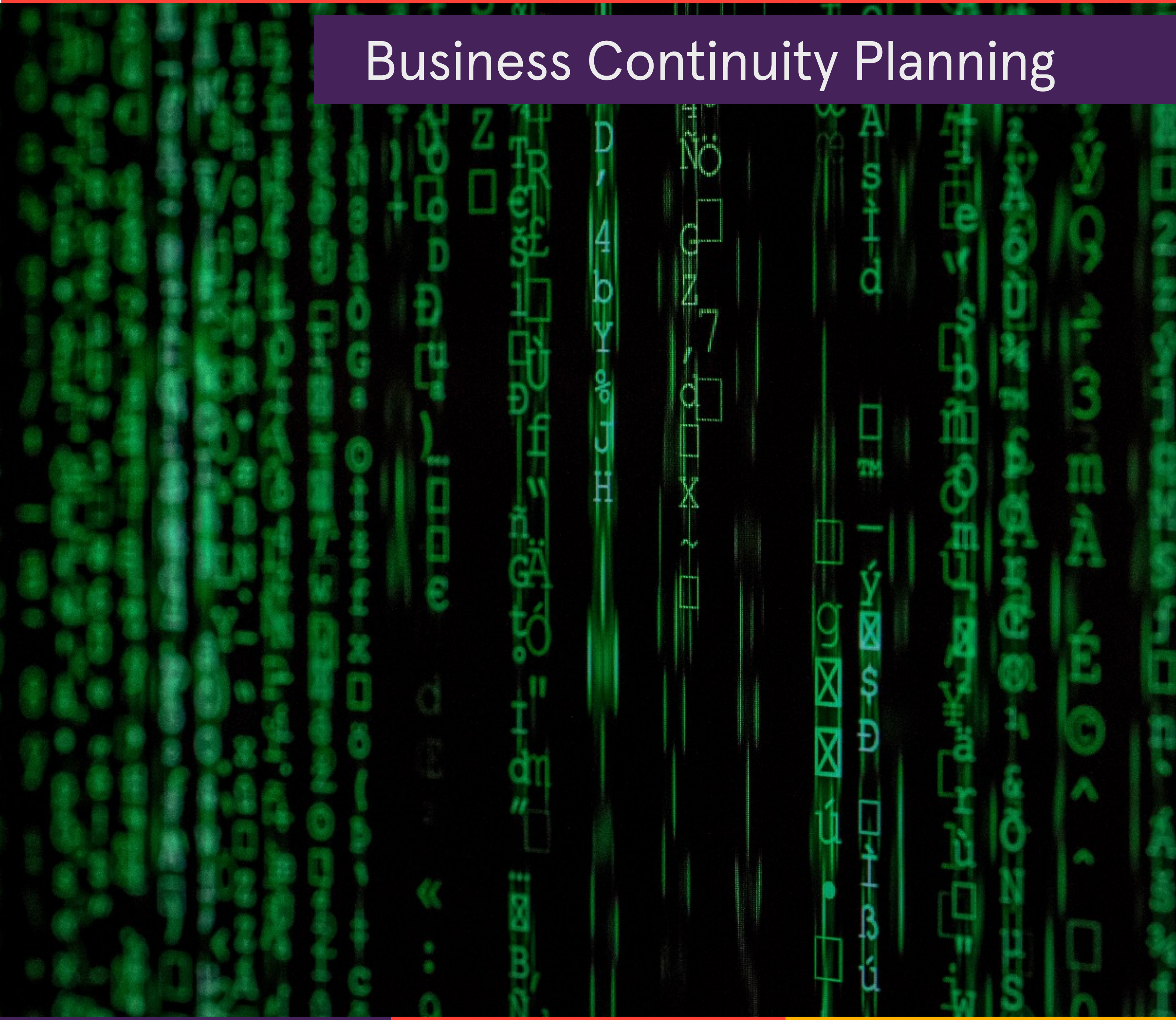
CIRRO

Toolkit
How To Plan Effectively for Disaster & Disruption

Business Continuity Planning



What to Plan

What To Ask

How To Recover

How To Create an Effective Business Continuity Plan

Following are some high level basic questions that can form a good internal discussions to understand your current situation, risks and requirements.

A good plan is one that is regularly reviewed, updated and has set test criteria against. Those organisations with ISO 27001 will have to provide evidence of Data Protection and Business Continuity. Cirro provides a number of services to support organisations from pure Back-up and DR to fully managed Business Continuity and Service Availability.

To create an effective Business Continuity Plan, start by working backwards and ask yourself some basic questions.

Step 1 - Prevention Is Better Than Cure

To begin planning, you need to know what you, who uses it and why, who manages it and how. How it is secure, where it is, where the back-up's up and how the are kept separate.

Audit, what do you have? How do you work? Get every department head to put this together. It should include every device and application used

Understand your process for managing those systems. Who administers them, how up to date are they. How are they backed-up.

Document and measure your risk profile. Understand and define 'normal' operations.

How educated and aware are your staff.

Step 2 - How Much Downtime Is Ok?

Each system, application or service will hold a different threshold of tolerance. You need to identify this by asking simple questions like this. You would have a different view of an issue if you knew the business was OK if a system was off-line for 48 hours than you would if it was for 30mins, and its 4pm on a Friday, or a critical time for your business.

Restore Time Objective (RTO)

The amount of time it takes to restore a system to working order

Step 3 - How Much Data Can You Lose?

Restore Point Objective (RPO)

The point in time of your last back-up which you will revert back to

You need to know the value of the data you hold in each system. This needs ton cover all ares, including any system of configuration changes.

If for example, it's a HR system, you might be OK to lose 5days of data, if it's mainly holiday requests and minor elements which can be fairly easily re-entered. However if it monitors peoples hours in real-time, that's not going to be good enough.

You need to keep in mind, if you have to go to a back-up, the data will only be as up to date as the last working, complete back-up. So if that was 1 hour or 1 week ago. That will probably have vastly different outcomes to your business.

Step 4 - Define Your Restore Priorities

It's important to run a number of scenario tests. In some ways, a 100% outage is easier to recover from, because you and a 100% restore. Usually tests are simulated and therefore don't reflect real-life.

So the reality is this; in what order should you restore services to have the minimum impact on your business?

Would this order change based on time of day? Day of the week, or at any seasonal time? A universities enrolment system will be low priority mid-term, but high priority during enrolment.

This might sound obvious when you think about it. But this aspect is rarely considered.

Step 5 - Where Can You Restore To?

This is the most overlooked part of Disaster Recovery, most organisations look at backing up data, but not at how or where it can be restored. This means that most organisations can only download a backup or restore it to an existing machine.

So, run through the above questions first, then ask yourself; how can we restore these data set's in this time, so that users can access them, suffering the data loss and restore times we have, and how will they access it?

The answers to these might surprise you, but this will give a good foundation for accessing the starting point of a DR and business continuity plan.

In terms of where, this is often the killer as many organisations complete pre-staged tests to restore backups to spare machines pre-build to a corporate standard.

This doesn't reflect the reality of a DR event and only demonstrates your organisations ability to restore a backup.

Step 6 - Key People & Weaknesses

The next stage is to understand WHO needs to do WHAT and WHEN to restore services and importantly, what and how do they communication with affected users.

The majority of organisation have an extreme reliance on very few key individuals or a 3rd party provider, to deliver services. This is naturally a potential risk. So assume they aren't available in your test scenarios.

We had a customer who was taking off-site back-ups on tape every day. He kept them at his house.

Naturally the company had a DR event when he was on holiday. He hadn't taken back-ups for several days, the last ones were locked in his house. He had to come back early from holiday. It took him years to recover.

Then he become a Cirro customer!

3, 2, 1, Rule For Data Backup

3 Copies of your Data

2 On at least 2 different media

1 copy off-site

Using Cloud Services (Declaration)

To be clear here Cirro provide Cloud Services, so you can read this as either:

1. We are trying to sell Cloud Services because thats what we do (and you are correct).
2. We have a lot of expertise in how to run back-up, restore, replication and continuity services from the Cloud, because thats what we do. For national rail & bus operators, for software providers and for SME's.

So declarations over!

Historically Cloud was good for keeping secure, remote, off-site back-ups. However, designed correctly, cloud can also offer a platform to restore your back-up to.

Meaning, you can spin-up a virtual server, deploy your back-up and recover, all in around 15mins to 2 hours (depending on what is already in place). That design lends itself well as a temporary, mid or long-term solution.

It is worth noting that many organisation use Cloud Software as a Service (SaaS), such as Office 365. Many of these services (including Office 365) do not have any back-up or Disaster Recovery capability, other than the resilience in its own platform.

17 Feb 2019 - Hackers wiped every server and every back-up of VFEmail, a secure email provider in the USA. With catastrophic loss of all data for 20 years.

Considerations & Scenarios

This is far from a definitive list, but some food for thought, these question will vary depending on your business, staff and suppliers.

- You can't get physical access to your primary office (and)
- You've lost remote access
- Your office equipment has been stolen or vandalised
- You've been hacked, how do keep your back-up's secure
- Someone has accidentally deleted or sent sensitive data to the wrong person (internal or external)
- Someone has an infected Desktop
- An important 3rd party provider become insolvent
- You lose connectivity or the service become degraded
- A main system or application fails at the worst possible time, when key staff are away
- You have a DDOS attack, Crypo-locker or Ransomeware attack

We have recently provided Cloud Backup services to an organisations, who's Cloud Backup provider become insolvent. They lost access to all previous back-ups.

17 Feb 2019 - Hackers wiped every server and every back-up of VFEmail, a secure email provider in the USA. With catastrophic loss of all data for 20 years.

More Questions...

- How many copies of your data should you keep and where? (see our 3,2,1 rule above)
- How frequently should you back-up and keep? (Every day, Every Week, Every Month for 3 months)
- How long do you need to keep data for?
- Are you backing up sensitive or personal data that falls under GDPR?
- How do you secure your back-ups and protect the data?
- How do you create a natural 'air gap' between your environment and your back-up data, so a hacker can't get it?
- If you get a ransomware attack, this are often timed, infecting your back-ups. How can you reduce this risk?
- What scenarios should you test? How can you make them real without having an impact
- Who will take responsibility for managing Business Continuity?
- Where will you keep you Back-up & DR policy so users can access it during a DR event?

Some Potential Pitfalls To Avoid

1. **Complacency** – this is important but only urgent when it's need. Get backups completed and test your ability to restore and make available to users
2. **Complacency** – keep updating the Business Continuity Plan to reflect business, system or personnel changes
3. **Understanding of Risk** – many budget owners don't understand the reality of business risk or the impact of a DR event, a small budget can go a long way

Asking these key questions will highlight your internal threats and weaknesses when it comes to protecting and preserving your data; helping you to create a comprehensive and effective Business Continuity plan.

Failing to plan is planning to fail. Start planning, build documentation, processes and priorities. Continue to understand and reduce your risk.

CIRRO

Cirro is certified to ISO 22301 for Business Continuity, ISO 27001 for Information Security and ISO 9001 for Quality and ISO 14001 for Environmental Management.

If you'd like to reduce your technology and operational risk, we'd love to help you.

You can find more advice, guides and tools on our website, including how to get in touch.

bsi. ISO 9001 Quality Management

bsi. ISO/IEC 27001 Information Security Management

bsi. ISO 22301 Business Continuity Management

bsi. ISO 14001 Environmental Management

You can find more advice, guides and tools on our website,
Need more help? Get in touch.