cit
Complete I.T.

Disaster Recovery

Creating an effective Business Continuity Plan

Contents

What is Business Continuity?

Business Continuity (BC) refers to maintaining business functions (or rapidly resuming them) in the event of a major disruption, whether caused by an environmental event, such as fire or flood, or by other factors, such as a malicious attack by cybercriminals.

What is a Business Continuity Plan?

A business continuity plan covers the way you plan and prepare for, and maintain critical business functions directly before, during and after a disaster; it covers business processes, assets, human resources, business partners and more.

The main reason companies implement a plan like this is because they want to remain able to provide their services or products to their customers.

If something happens and you are not able to deliver to your customers, there is a risk that they will simply go to another company. This will obviously cause you to lose not only customers, but valuable income, some of which may be needed to further recovery.

Isn't it just a new name for Disaster Recovery?

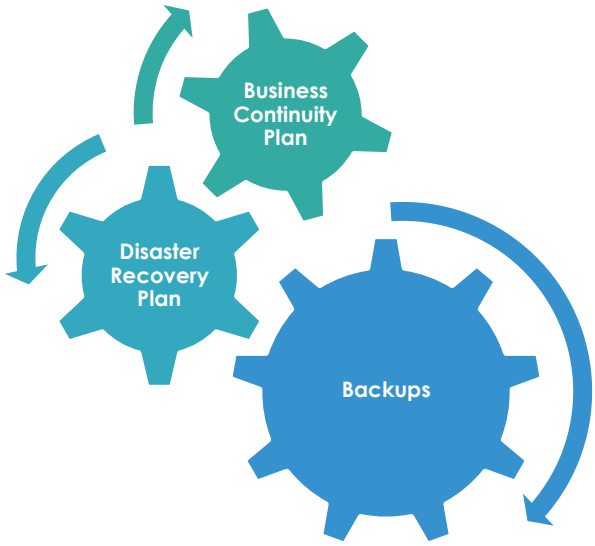
Many people think a disaster recovery (DR) plan is the same as a business continuity plan, but a DR plan focuses on the specific process of recovering the facilities, operations and resources lost during the disaster, to bring the business back to full functionality.

Business Continuity extends this concept to preparing for the business being able to carry on working, even in a limited operational capacity, during the initial disaster and the entire recovery process. As a result, it requires more preparation and planning, and also more resources to be available in order to be effective.

To this end, the Disaster Recovery Plan forms only a part of a Business Continuity Plan.

Backups, Disaster Recovery, Business Continuity…

Your critical files, whether they're accounts, customer data, orders and shipments or e-mails, all need to be backed up. In the event of a loss of any of those critical files, they can then be recovered from backup. From an I.T. perspective, this is the foundation on which Disaster Recovery and Business Continuity are built. Without backups, you have nothing to recover in the event of a disaster, and without your critical files being available, your business will be unable to operate.



So, what's the difference?

Backups are current duplicates of your files and applications (and systems, too) which you can recover either individually or en-bloc should you need to.

Disaster Recovery is the process which your business would follow to get back to full operational capability after an incident, but focuses on what happens after the disaster, and is generally of a technical nature. A business may have multiple DR Plans, for example for premises and facilities, as well as I. T. (ITDR).

Business Continuity, as stated earlier, is an evolution of Disaster Recovery, and covers the way a business plans for and maintains critical business functions, directly before, during and after a disaster.

It may be well to consider a BCP as an umbrella plan, with DR a part of it. Without a DR component to the BCP, there is a good chance the whole strategy may be ineffective.

On the other hand, DR can actually stand alone, and many business can manage just fine without a BCP.

If a Business Impact Assessment indicates your business model is structured in such a way that it can withstand an interruption in business flow to deal with a disaster and its aftereffects, including recovery, then you may not need to consider a BCP, but you should have a DR Plan in place.

Consider these 3 scenarios

1. Accidental Deletion James is a Sales Manager. He has a presentation to the executive level coming up in two days and has been working for two weeks on his projections, presentation, and reports. He gets to work in the morning to find that the entire folder containing these critical files has disappeared. He eventually finds out that the folder was accidentally deleted last night.

   James' company run backups throughout the day. James is able to call on his IT Support team to arrange for the relevant folder and all the files from the mid-day backup to be restored to their original location, so he can carry on with his preparations for the meeting.

2. The tenant on the floor below you catches fire Your employees arrive at work in the morning, to find that there are fire engines and fire crews all-round the building, water everywhere, and the smell of burning in the air. The tenant company in the building below you had a fire break out at 1 am, and it has gutted the building from their floor up.

   Everyone has their laptop with them, but the servers, the network, the filing cabinets, and the onsite backups are all gone.

   Thankfully, the offsite backups were complete at 11:30 last night. However, you currently have no way of getting to them. You implement your disaster recovery plan, to sort out a temporary workplace, and getting access to those files.

   In this situation, in order to be able to access and use these critical files from the offsite backups, new servers will need to be sourced, built & configured, installed, and the data restored to them. This is not going to take hours, this is going to take days, if not weeks. However, these time estimates have been built in to the company DR Plan, which is now enacted, in order to be able to sort out a new workplace, and somewhere for the servers to go in order for your teams to be able to access them once they are ready.

3. Ransomware attack cripples your network It happens to all of us. A particularly nasty piece of malware gets past your network defences and wreaks havoc across your network. All your critical files are encrypted, and this includes the onsite backups. Your business cannot afford to have its operations interrupted for anything less than 4 hours.

Thankfully, you have a Business Continuity Plan in place to deal with this. In this case, you call on your IT Support to begin troubleshooting and tracking down the source of the infection, and they take your servers offline. You have a core group of BCP laptops which are not normally connected to the network but are regularly tested and updated in order to be used in such an emergency.

Your I.T. Support works in two teams, with one team tasked with cleaning the network of the malware infection, and the other with bringing your backup servers online at the same time. With a cloud hosted server solution, you are able to get your core critical business functions house offsite away from the network, logged in and accessing the servers independently of your main business premises. They are able to carry one the business operations while the rest of your employees assist where they can with the IT Recovery.

Eventually, the system is cleaned, all of the infected and encrypted files are removed, and the IT Support team restore all your data files, including the ones which were worked on during the clean-up phase. Your business has continued to operate throughout the entire recovery, which may have taken days to complete.

What should your DCP or BCP Contain?

While these plans are slightly different, they do share the same common goals – to offer support and assistance during a disaster. Therefore, regardless of what type of plan you decide to adopt, there are common elements both need to incorporate in order to be successful.

1. An operational plan for potential disasters that could happen in your geographical area.

2. A succession plan for you or your top management.

3. Employee training and cross-training. Your employees should know their role in the plan and be trained in other responsibilities should someone else be unable to perform their role.

4. A communication plan that includes ways of communicating if networks are down.

5. Off-site locations for staff and managers to meet and work.

6. A focus on safety. Foster partnerships and communication with local and emergency response services. Ideally, all employees should at least know basic first aid. Employees who are members of local Emergency Response Teams make great team leaders.

7. Daily backups of your systems and data. Be sure to also train staff in the testing and recovery of systems.

8. Training and testing of all employees to practice recovery activities in realistic role-playing scenarios.

9. Regular audits and updates of your plans to ensure they are still relevant and able to protect your systems and company.

In addition to these plan components, your overall BCP Strategy should also include investment in systems design to specifically assist in managing and aiding a recovery, especially of I.T. systems.

With a plan that is carefully prepared, tested, and updated on a regular basis, you should be able to better weather any disaster. If you are looking for information on how to develop or improve your plans get in touch with us today.

7 Key principles of Business Continuity Planning

1. Get your employees involved

A BCP will only be successful if everyone understands it. Employees are an invaluable source of ideas and insights into how your business may be affected by a disaster. You should communicate your BCP to your employees regularly, and actively solicit their input.

2. Keep your customers in the loop

Customers are the lifeblood of every business, and should be treated as such even during a disaster. Communicating with your customers by sending e-mail, notices on the company website and social media, along with text messages to key contacts' phones are all good ways for a business to express concern about how the disaster may be affecting their customers. That level of communication and customer service can possibly even help turn a disaster into an opportunity for better long-term customer loyalty.

3. Collaborate with your suppliers

Businesses increasingly work in tightly interdependent networks of suppliers and partners. By working collaboratively with these 3rd parties, your business can make itself more resilient and better protected against disasters.

4. Periodically test and update your Business Continuity Plan

All too often a Business Continuity Plan is drawn up and set on paper, and there it stays. Assumptions about a plan should be validated through regular testing, and it should also be continuously updated to take into account any changes in the business.

5. Compliance needs to be factored in

Whether it's GDPR, PCI-DSS, Cyber Essentials, or any industry-specific Regulatory Authorities, your business will be subject to certain regulations which may mandate a certain level of disaster preparedness, but will almost certainly mandate reporting in the event of a disaster. A specific example is reporting to the Information Commissioners office in the vent of a data breach under GDPR Regulations. The HSE (Health & Safety Executive) may be particularly relevant in regards to workplace safety in the affected premises.

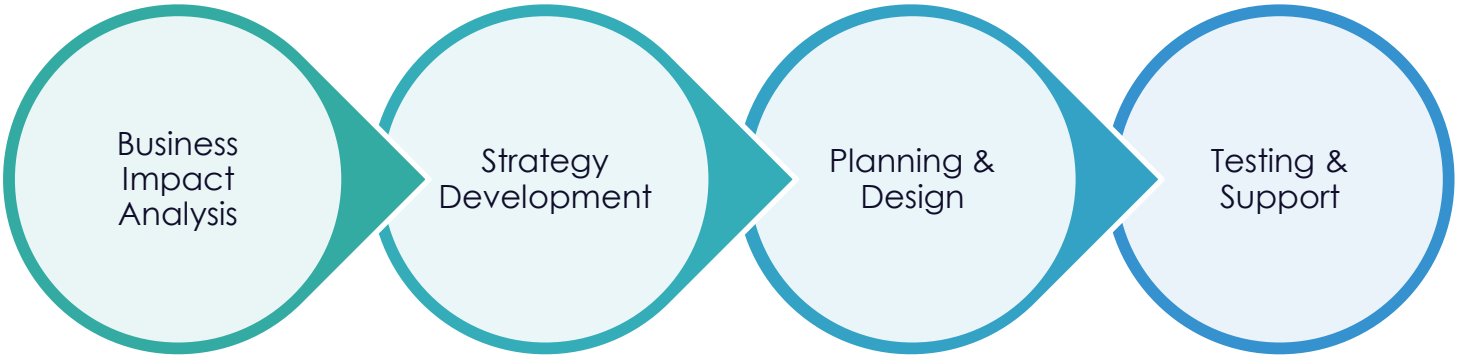
6. Examine your insurance options carefully

Insurance coverage varies greatly, and navigating complex polices can get confusing, especially in the wake of a real-time disaster. Businesses have to exercise careful legal and financial diligence to ensure their policies cover all aspects of disaster recovery and revenue loss, not just the initial damage repairs. In some cases, it may be prudent to look into obtaining contingent business interruption insurance.

7. Data backups are NOT enough

Many businesses think they're safe just because they've backed up their critical files. The problem is that those files depend on applications and systems running on certain hardware in order to be of any use. In the event of a disaster, you need to be able to get to those critical files, as well as having the systems in place to be able to use them.

Steps to creating a Business Continuity Plan



- Assessment of present BCP
- Interviews with key staff
- Determining RTO/RPO for each Dept

- Risk and threat assessments
- Critical Process Identification
- Critical timing identification

- Key business areas
- Incident response plan
- Key personnel

- Regular Testing of BCP
- On-site Technical Support
- Remote Technical Support

Business Impact Analysis

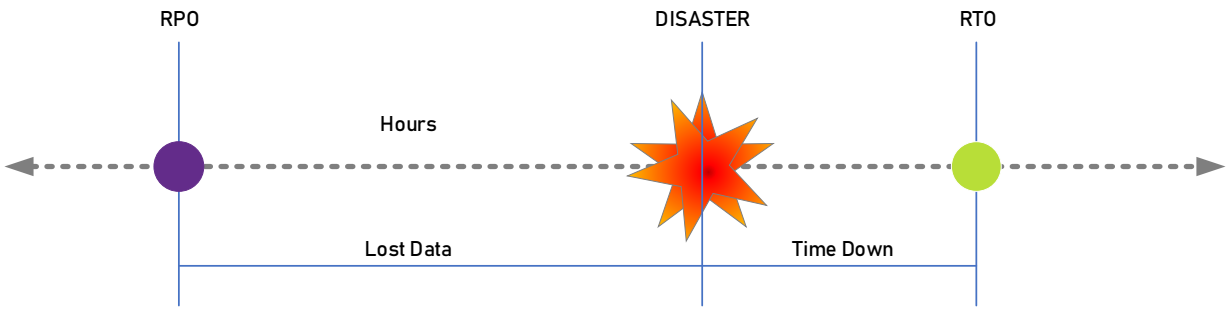
The first and quite possibly lengthiest step is to conduct a Business Impact Analysis(BIA).

A BIA identifies the impact of a sudden loss of business functions, usually quantified in a cost. Start by assessing your business processes, determining which areas are vulnerable, and the potential losses if those processes suddenly become unavailable. This should be carried out with interaction from key members of staff/department heads.

Such analysis also helps you evaluate whether you should outsource non-core activities in your BC plan, which can come with its own risks. The BIA essentially helps you look at your entire organisation's processes and determine which are most important.

What information do you need in your Business Impact Analysis?

Key information you should determine for each department to assist in determining your critical processes is the RTO/RPO Information for each department.



RTO stands for Recovery Time Objective. It's a metric that helps to calculate how quickly you need to recover your IT infrastructure and services following a disaster in order to maintain business continuity. It is measured in terms of how long your business can survive following a disaster before operations are restored to normal. If your overall RTO is twenty-four hours, it means you've determined that the business can maintain operations for that amount of time without having its normal data and infrastructure available. If data and infrastructure are not recovered within twenty-four hours, the business could suffer irreparable harm.

RPO, or Recovery Point Objective, is a measurement of the maximum tolerable amount of data to lose. It also helps to measure how much time can occur between your last data backup and a disaster without causing serious damage to your business. RPO is useful for determining how often to perform data backups.

RPO is significant because in most cases, you will likely lose some data when a disaster occurs. Even data that is backed up in real-time has a risk of some data loss. Most businesses back up data at fixed intervals of time -- once every hour, once every day or perhaps as infrequently as once every week. The RPO measures how much data you can afford to lose as the result of a disaster.

Difference between recovery Objectives

RTO and RPO are both business metrics that can help you calculate how often and how to perform data backups. However, there are some key differences:

- **Assessment basis.** RTO reflects your overall business needs. It's a measure of how long your business can survive with IT infrastructure and services disrupted. In contrast, RPO is just about data. It determines how often to back up data and does not reflect other IT needs.

- **Cost relevance**. The costs associated with maintaining a demanding RTO may be greater than those of a granular RPO. That's because RTO involves your entire business infrastructure, not just data.

- **Automation**. Meeting your RPO goals simply requires you to perform data backups at the right interval. Data backups can easily be automated, and an automatic RPO strategy is therefore easy to implement. RTO, on the other hand, is more complicated because it involves restoring all IT operations. It is virtually impossible to achieve RTO goals in a completely automated way (although you should automate as much of your recovery process as possible).

- **Ease of calculation**. In some ways, RPO is easier to implement because data usage is relatively consistent and there are fewer variables. Because restore times involve your entire operation, not just data, it is more complicated. Restore times can change based on factors such as the time of day or the day of the week at which a disaster occurs. The RTO must be aligned with what is possible by the IT organization. If the minimum restore time possible is 2 hours, then an RTO of 1 hour will never be met. It administrators must have a good understanding of the speeds with which different types of restores can take place. Only then can an RTO be properly negotiated and met based on the needs of the business owners.

RTO, RPO and DR/BC planning

To build a disaster recovery or business continuity plan that guarantees the survival of your business after a disaster and is also cost-effective, you need to determine viable RTO and RPO figures. You need to ensure that you can achieve both RTO and RPO goals in order to recover effectively from a disaster.

Risk Assessment

Once you have your RTO/RPO Assessment for each department you need to determine how at risk each department is, and this also starts with a Risk Assessment for the entire busines.

Performing a specific Business Continuity Management related Risk Assessment helps you consider the various in-scope resources and the risks to them.

For example, premises ar risk of flooding, are there controls that could be put in place, or should relocation be a serious consideration?

Example 2; Are your IT Security measures adequate/acceptable? What routine measures can be taken to reduce the risk of cyber attack/document loss (such as replacement UTM Device/Firewall or a better backup solution, and what should be considered as part of a Business Continuity Plan, to be enacted in an emergency? And what measures may form elements of both?

Plan Development

With the information gathered during your Business Impact Analysis and having determined the risks to the business and/or departments, You can begin to develop your plan.

This can be as comprehensive or as brief as it needs to be, but must include;

1. **Scope** – the plan must state what is within the scope of the BCP, and what measures are out of scope.

2. **Key Personnel** – who is responsible for enacting and managing a BCP Response to an event, department heads, Who is reaponsible for testing and maintenance of the plan etc.

3. **Key business areas** – such as finance, payroll, ordering and shipping.

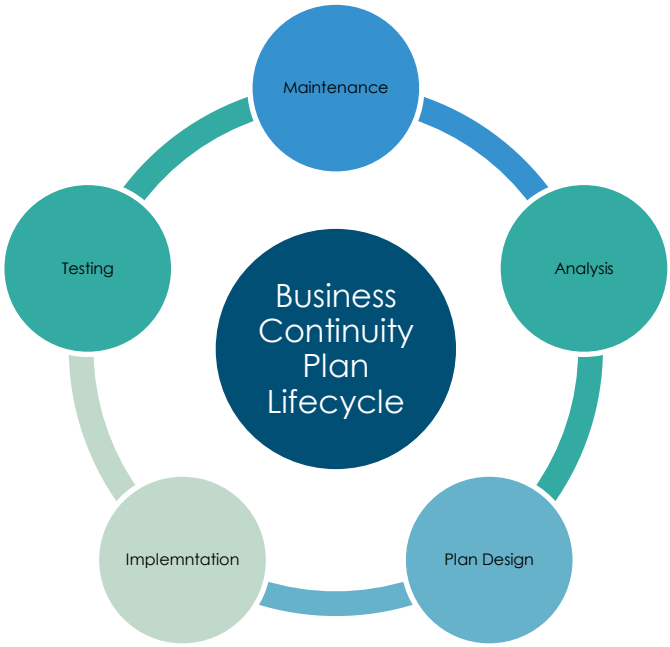
4. **Critical functions** – accounts, e-mail, shared files etc.

5. Identified **dependencies between business areas and critical functions**. E.g. Finance Dept MUST have access to the accounting software.

6. Identified **acceptable downtime for each critical function**. E.g. e-mail MUST be running within 2 hours.

7. **Key Information**; One common business continuity planning tool is a checklist that includes supplies and equipment, the location of data backups and backup sites, where the plan is available and who should have it, and contact information for emergency responders, key personnel and backup site providers.

Implementation & Maintenance



Testing and Measuring

Testing a plan is the only way to truly know it will work. Obviously, a real incident is a true test and the best way to understand if something works, however at the risk of the plan not working, it doesn't help you with the current event.

A controlled testing strategy is much more comfortable and provides opportunities to identify gaps and improve the plan.

Testing Frequency & Depth

Many organisations test a business continuity plan two to four times a year. The schedule depends on your type of organisation, the amount of turnover of key personnel and the number of business processes and IT changes that have occurred since the last round of testing.

Common tests include table-top exercises, structured walk-throughs and simulations. Test teams are usually composed of the recovery coordinator and members from each functional unit.

- A table-top exercise usually occurs in a conference room with the team poring over the plan, looking for gaps and ensuring that all business units are properly represented.

- In a structured walk-through, each team member walks through his or her components of the plan in detail to identify weaknesses. Often, the team works through the test with a specific disaster in mind. Some organisations incorporate drills and disaster role-playing into the structured walk-through. Any weaknesses should be identified, corrected and an updated plan distributed to all pertinent staff.

- It's also a good idea to conduct a full emergency evacuation drill at least once a year. This type of test lets you determine if you need to make special arrangements to evacuate staff members who have physical limitations.

- Lastly, disaster simulation testing can be quite involved and should be performed annually. For this test, create an environment that simulates an actual disaster, with all the equipment, supplies and personnel (including business partners and suppliers) who would be needed. The purpose of a simulation is to determine if you can carry out critical business functions during the event.

During each phase of business continuity plan testing, include some new employees on the test team. "Fresh eyes" might detect gaps or lapses of information that experienced team members could overlook.

Employee Awareness & Training

Much effort goes into creating and initially testing a BC plan. Once that job is complete, some organisations let the plan sit while other, more critical tasks get attention. When this happens, plans go stale and are of no use when needed.

Technology evolves, and people come and go, so the plan needs to be updated, too. Bring key personnel together regularly to review the plan and discuss any areas that must be modified.

Prior to the review, solicit feedback from staff to incorporate into the plan. Ask all departments or business units to review the plan, including branch locations or other remote units. If you've had the misfortune of facing a disaster and had to put the plan into action, be sure to incorporate lessons learned. Many organisations conduct a review in tandem with a table-top exercise or structured walk-through.

This keeps employees and staff aware of the plan, and allows you to conduct training as part of the testing elements to ensure not only are staff aware of the plan, but how it is to be used and possibly even their roles in it.

Management is also key to promoting user awareness. If employees don't know about the plan, how will they be able to react appropriately when every minute counts? Although plan distribution and training can be conducted by business unit managers or HR staff, have someone from the top kick off training and punctuate its significance. It'll have a greater impact on all employees, giving the plan more credibility and urgency.

Investment in control measures and plan elements

Sometimes, the development of a BCP highlights areas where investment may be needed, whether it is in better I.T. Security, or even budgeting for alternative premises. If this is the case, be prepared to make a case for this additional expenditure, using the results of the BIA and Risk Assessments for the BCP as justification.

3rd-party support

Developing a comprehensive DR Plan or BC Plan will take time and effort. There are numerous resources available to you to help with this, from Business Continuity Consultants to Online Plan resources and guidance, regulatory bodies' guidance, and of course us here at Complete I.T.

We can also involve the hardware vendors, such as Dell and HP, when it comes to dealing with replacement hardware, or spare computers and I.T. Infrastructure devices.

It should also go without saying that Complete I.T. are here to provide onsite and remote support when actively dealing with a DR or BCP incident, in order to get you back up and running as quickly as possible.

Control

Controlling the distribution of your plan documentation

It is vital to the integrity of your Business Continuity Plan that all copies of the plan are controlled, and through testing and maintenance all copies have changes and amendments managed. You should establish control measures to ensure that out of date copies or uncontrolled copies are removed from circulation, as having the incorrect or outdated information may make your response to an incident that much less effective.

Management of key personnel and resources

Where staff who are key personnel with regards to the BCP change, the Plan needs to be updated to reflect the changes, and appropriate training should be arranged for the incoming staff who will become key personnel.

Also, whenever amendments are made to the BCP, these changes should be passed on to key personnel immediately.

Management of resources

Where planned-for resources are held, such as emergency I.T. Equipment (laptops, cold backup servers, etc) these must be maintained in accordance with I.T. best practice as your live IT Infrastructure.

Other resources – torches, radios etc should also be subject to regular checks and maintenance where required.

Summary

Backups, Disaster Recovery and Business Continuity

Business Continuity Planning incorporate a Disaster Recovery Plan, but extends it to prepare for keeping the business running before, during and after the disaster. A major element of both with regards to I.T. is comprehensive, reliable and usable backups.

Business Impact Analysis and Risk Assessments
Business Continuity and Disaster Recovery Planning both require an analysis of the business process and an assessment of the risks and threats posed to each business process by possible disaster events or incidents, Carrying out a Business Impact Analysis and Threat Risk Assessment provides you with the details to be able to formulate your response plan.

Buy-in from key stake-holders
A successful BCP must involve all employees and key stake holders to ensure everyone knows what the plan is, and who is responsible in the event of an incident occurring, as well as providing a source of information and ideas on formulating the plan to begin with.

Implementation and Awareness
Once developed and approved, the plan should be implemented, and all employees informed through training. Key personnel can assume their responsibilities with regards to the plan, and can prepare for testing.

Continuous Development and regular testing
A stale plan which is created and left becomes useless. Only through regular testing can the plan be proven, and problems/gaps discovered for which amendments can be made and applied to ensure the plan stays current and relevant.

How can Complete I.T. help?

It is vitally important to note that whilst a Disaster Recovery Plan generally applies to a single technical aspect of the business (and in general, this is I.T.), a Business Continuity Plan encompasses all of this and more, and should deal with all aspects of keeping the business running.

Complete I.T. appreciate that a significant part of this planning will revolve around your core I. T. services and infrastructure, and our team of Technical personnel will be on hand to help you achieve your objectives with advice, consultancy and equipment, when drawing up your DR or BC Plans.

Our partnerships with Datto for their Alto and Siris Backup devices, and Microsoft for their Microsoft 365 and Office 365 Cloud hosted productivity tools and file storage, for example, form a core part of our own BCP offering, as this technology allows our clients to develop not only a business continuity plan, but a resilient, robust and protected I.T. infrastructure on which to run their core business processes.

Our Partnerships

Datto Data Backup and Disaster Recovery devices

Siris – All-in-one Business Continuity solutions
https://www.datto.com/continuity/siris

Alto – Total Data Protection for SMBs
https://www.datto.com/continuity/alto

Microsoft Cloud Hosted Productivity

Microsoft 365 Business
https://www.microsoft.com/en-gb/microsoft-365

Office 365
https://products.office.com/en-gb/compare-all-microsoft-office-products?tab=2&OCID=AID679471_OO_HLW_mscomrefresh

Further research and reading

Disaster Recovery Plan templates:

https://www.probrand.co.uk/blog/pb/october-2018/it-disaster-recovery-plan-templates
https://www.business.hsbc.uk/en-gb/gb/article/qa-disaster-recovery-planning

Business Continuity Planning resources:

https://www.gov.uk/government/publications/business-continuity-planning
https://www.techopedia.com/definition/3/business-continuity-plan-bcp

Or, you can speak to your **Complete I.T. Team** of Technical Consultants, Account Managers and Helpdesk Analysts who will be able to help you find further information on Business Continuity and Disaster Recovery Planning.

Glossary

Backup Process to ensure critical data and programs are available in the event they are destroyed/deleted.
BC Business Continuity
BCP Business Continuity Plan
BIA Business Impact Analysis
DR Disaster Recovery
DRP Disaster Recovery Plan
RPO Recovery Point Objective – how old your backed up data is at the point of recovery.
RTO Recovery Time Objective – how long a process can be down for before it starts to become a problem
UTM Unified Threat Management – perimeter firewall device to protect your IT network

References

UrbanNetwork 7 Key Principles of Business continuity for Business, Mar 15, 2018
MSP360 Blog RTO vs RPO The Difference