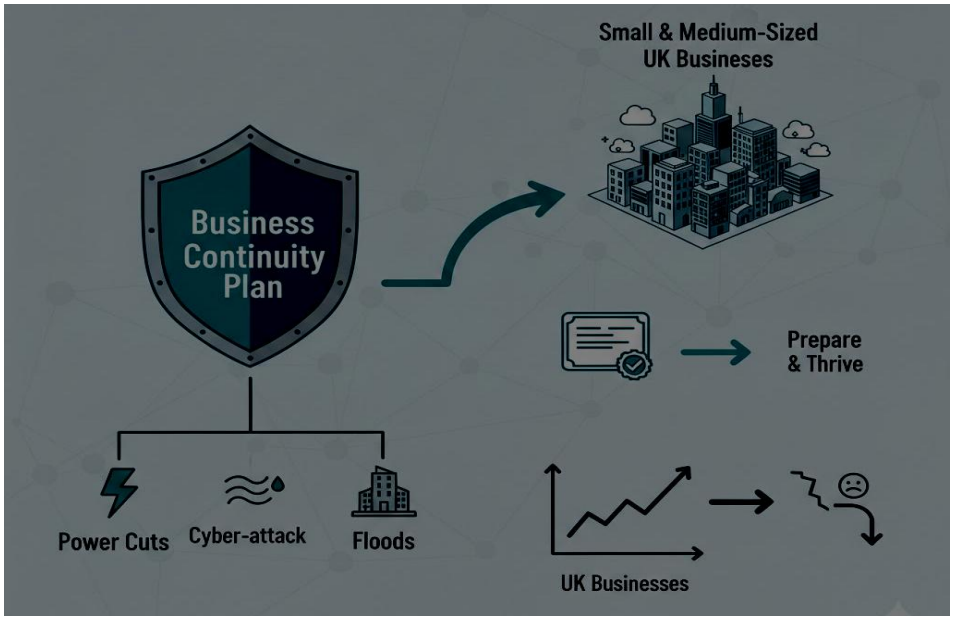
Business Continuity Plan Template

why continuity planning matters

- A Business Continuity Plan (BCP) is a basic document that allows your business to continue functioning in case there is some type of crisis.
- It is a way for your business to be prepared for different situations such as, a cyber-attack, floods, power cuts, or a key member of staff gets ill.
- Small and medium-sized businesses throughout the United Kingdom are at risk of being versus a variety of threats more often than many people may realise.
- Having no BCP can result in even a small problem causing a loss of revenue when dealing with unhappy customers.
- A BCP identifies the critical areas of your business.
- It will provide you with a way of thinking about potential problems your business may encounter and how to respond while mitigating the issue.
- A BCP does not have to include a detailed document, it only needs to be relevant, easy to read, and implementable.
- Having a BCP can help you achieve Cyber Essentials certification.
- If you have a data incident, having a BCP can demonstrate that you have put "appropriate measures" in place for the UK GDPR requirements.
- The BCP will create a working continuity plan without requiring costly consultants or several weeks of work.



What is a Business Continuity Plan?

A Business Continuity Plan (BCP) is a document that allows you to explain:

- What your business will do to continue to run after the major interruption has occurred and/or during the major interruption.

A BCP is designed to ensure that critical services will continue to operate when there is no access to:

- Systems
- Buildings
- Staff
- Suppliers

A BCP will answer some of the following practical questions:

- Who will declare an incident or a disaster?
- Who will make management decisions?
- Who will ensure that we continue to provide services to clients?
- When will we restore Services?
- What type of communication will we have when communicating with our clients?

A BCP is NOT:

- An IT document only.
- A 100-page document that no one reads.
- An assurance that everything will be OK.

A BCP is simply a clear, well-documented process for managing a disruption and getting back to business as normal as soon as possible.

Every SME with 5 to 250 employees will benefit from having a BCP in place to ensure the continuity of their business.

Business Continuity vs Disaster Recovery explained simply

There tends to be confusion around these two phrases.

Business Continuity

Refers to maintaining business operation during times of disruption.

Examples Include:

- Working remotely when there's a flood
- Manually running invoices while systems are being restored
- Switching to an alternative supplier

Disaster Recovery

Refers to the ability to restore systems and data after an incident occurs.

Examples Include:

- Restoring from backups after a ransomware attack

- Rebuilding servers
- Recovering from cloud network/device outages

Cybersecurity

Refers to measures taken to reduce the risk of an incident occurring.

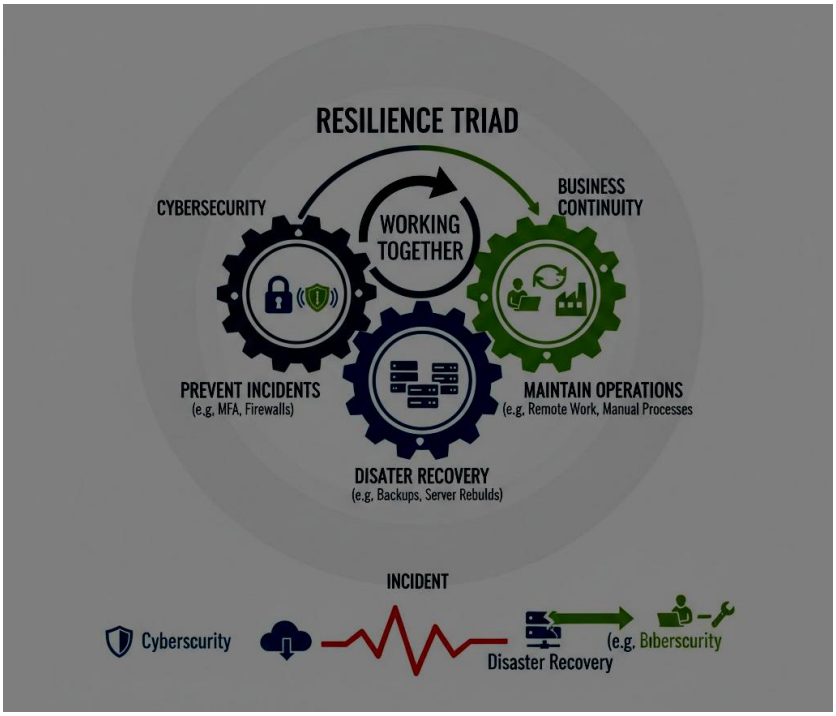
Examples include:

- Using multi-factor authentication
- Installing a firewall
- Endpoint security controls
- Complying with Cyber Essentials security requirements.

All of the above three areas (cybersecurity, disaster recovery and business continuity) work in conjunction with one another:

- Cybersecurity helps prevent an incident from occurring,
- Disaster recovery restores systems after an incident has occurred,
- Business continuity enables you to continue trading while recovering from an incident.

Without continuity planning, IT recovery in isolation is insufficient.



What happens when SMEs do not have a plan

Common consequences of disruption when a plan is not in place include the following:

Financial loss:

- Lost revenue as a result of downtime
- Contract penalties
- Emergency IT costs
- Overtime/temporary employees

reputation Damage:

- Resilience is expected by clients; silence during disruption severely damages trust.

Regulatory exposure:

In the UK, under the GDPR, organisations must have appropriate resilience and availability of personal data. If the disruption causes the following to occur:

- Loss of data:
- Delay in breach notification
- Extended unavailability of personal data

then the Information Commissioner may take action.

This is not legal advice, but the expectation of resilience is on the rise.

Insurance complications:

Cyber insurers are increasingly seeking evidence of the following:

- Documented evidence of tested backups:
- Incident response plans
- Certification from Cyber Essentials

If documentation is not provided, claim payouts are subject to scrutiny.

Leadership stress:

- The decision-making process and forms of communication are delayed due to lack of plans, resulting in low staff confidence.

A BCP will provide some reassurance and help alleviate panic.

Step-by-step guide to building a BCP

Step 1: Assign Ownership

Select a senior individual to oversee the development, ongoing activation, and maintenance of the business continuity plan.

Step 2: Identify Critical Functions

Identify those key activities required to continue business operations for the purposes of ensuring revenue streams, maintaining compliance and providing for customer service.

Step 3: Execute Business Impact Analysis (BIA)

Determine how disruptions to each critical function would impact the organisation in terms of its financial viability, reputation and operational capacity.

Step 4: Identify Risks

Identify all realistic, credible risks to your organisation, including but not limited to cyber attacks, information technology failure (IT), fire, flooding or major supplier disruption.

Step 5: Specify Recovery Objectives (RTO/RPO)

Establish measurable recovery objectives for both time to restore systems and functions and the amount of data to be restored.

Step 6: Create IT Recovery Plan

Document how your company's systems, applications and data will be restored and what the backup and responsibilities for each are.

Step 7: Create Communication Plan

Determine how to communicate to employees, customers and suppliers during and after a disaster.

Step 8: Explore Alternative Work Arrangements

Develop practical alternatives for employees to continue their work responsibilities, including remote working arrangement, temporary office locations or prioritising workloads.

Step 9: Write and Distribute

Document the BCP and ensure that employees are aware of where it is located and how to access it.

Step 10: Test and Update

Test the BCP through regular or scheduled testing (exercises) and update the plan to reflect any changes in business processes or technology.

Fully structured Business Continuity Plan template (fillable format)

1) Document Control

- Version
- Date Created
- Date Reviewed
- Plan Owner
- Approved By

2) Business Overview

- Business Name
- Employee Count

- Business Location
- Primary Services Provided
- Key Suppliers
- Key IT Systems

3) Business Impact Analysis

- Functional Area of Business
- Function/Area of Business
- Maximum Acceptable Downtime of Business Function
- Cost to Business if Function Disrupted
- Company Reputation if Function Disrupted
- Regulation of Business Function
- Level of Priority for this Function

4) Risk Assessment

- Risk in Business
- IT System Outage
- Cyber Attack
- Fire/Flood
- Power Failure
- Employee Non-Availability
- Supplier Non-Availability
- Impact of Risk Assessment
- Likelihood of Occurrence
- Impact of Each Risk in Business
- Control in Place (i.e. Process, Policy, Procedure)
- Further Action Required

5) Incident Response Structure

Roles:

- Incident Lead
- IT Recovery Lead
- Public Relations Lead

Escalation path:

- Internal Escalation Process of Incident
- External Escalation (Insurance Company, IT Support Provider)

6) IT and Data Recovery

- Backup Provider
- Frequency of Backups
- Backup Storage Location
- RTO
- RPO
- Date of Last Backup Test

7) Communications Plan

- **Internal:** Staff Notification Process
- **External:** Are Template Notification Messages Prepared
- **Suppliers:** Are Contact Lists Current
- **Media :** Is Company Spokesperson Known

8) Remote Work Plan

- Laptops Available
- VPN Capability
- 2FA Enabled
- Procedures for Secure Remote Access

9) Alternative Worksites

- Secondary Location
- Temporary Office Providers
- Working from Home Policy

10) Testing and Maintenance

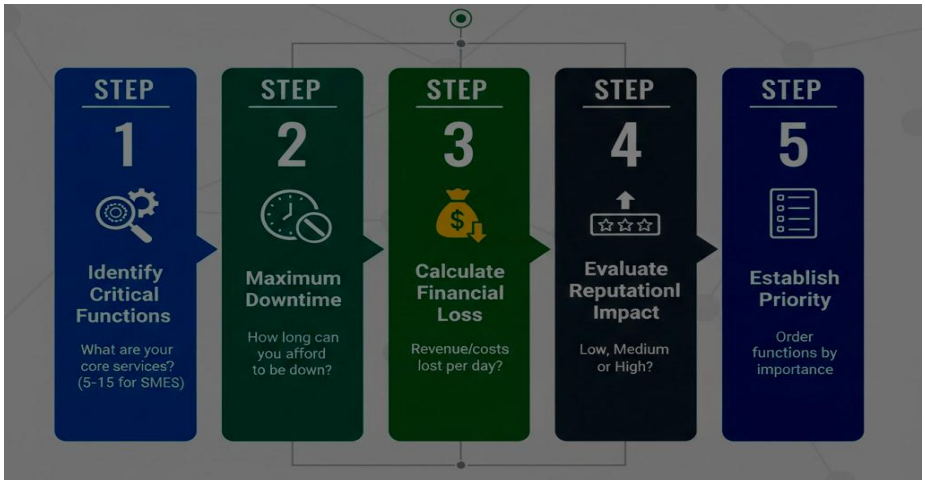
- Next Test Date
- Type of Test
- Frequency of Plan Reviews
- Specific Event(s that will Trigger Review of Plan

Business Impact Analysis

There are five steps to writing a simple business impact analysis:

- Identify the critical functions performed by your business.
- Identify the maximum amount of downtimes can your business afford?
- Calculate the amount of money you could lose each day if your critical function was not available.
- Evaluate how your business will be impacted reputationally (low, medium or high).
- Establish the priority of your critical functionalities.

The majority of small to medium size enterprises (SMEs) can identify 5 to 15 critical functions.



Simple Continuity Checklist

☐ Appoint an owner of the business continuity plan

☐ Identify the critical business functions

☐ Identify dependencies

☐ Complete a BIA (Business Impact Analysis)

☐ Document risk analysis

☐ Define responsibilities for incidents

☐ Document backup strategies

☐ Test backup strategies

☐ Define RTOs (Recovery Time Objectives) & RPOs (Recovery Point Objectives)

☐ Review existing Cyber Risk Insurance

☐ Consider if your business is Cyber Essentials compliant

☐ Secure access to your network remotely

☐ Identify alternative suppliers of critical products and/or services

☐ Develop communication templates

☐ Test business continuity plans within 12 months

FAQs

1. Is a business continuity plan legally required in the UK?

Not as a general rule; however, the UK General Data Protection Regulation (GDPR) imposes an obligation on businesses to have appropriate and proportionate technical and organisational measures in place to ensure the availability of any personal data.

2. How often should a business continuity plan be reviewed?

At least annually or when there has been a major change.

3. How long will the business continuity plan be?

The majority of small to medium size enterprises (SMEs) can develop a plan of approximately 10 to 25 pages in length.

4. Who owns the business continuity plan?

A senior member of management of the organisation.

5. Is a business continuity plan just for large enterprises?

No, small enterprise is generally more vulnerable to any business interruption.

About This Guide

This guide has been produced by **Computer Support Centre.** We are a managed IT Services Company that also provides business resilience consultancy, primarily to SMEs throughout the UK.

The contents of this guide have been developed based upon our extensive experience in assisting organisations improve their IT Resilience, achieve compliance requirements including UK GDPR and Cyber Essentials as well as prepare for operational disruption.

In conclusion, the objective of this guide is to assist UK organisations in developing business continuity plans that are useful, easy to read and provide true protection, as opposed to complex, theoretical solutions.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit our official website:
 https://computersupportcentre.com

© **Computer Support Centre**

Conclusion

A BCP is intended to protect your ability to continue to trade as disruption occurs and is about protecting that ability, not producing an unnecessarily complicated document. Disruption can be caused by many different things, including; ransomware, flooding, supply chain failure, or a lengthy

power cut. By having a practical, tested plan in place, you will reduce your downtime, protect your revenue and create reassurance for your clients.

Continuity Planning does not have to be complicated for SMEs in the UK, it should simply be realistic, documented and regularly reviewed. The organisations that have the fastest recovery are not those that experience no disruption, but those that are prepared for disruption.