Business Continuity Guidance for Businesses and Voluntary Organisations

This page has been left blank intentionally

Business Continuity Guidance for Businesses and Voluntary Organisations

Be Prepared

Business Continuity Management (BCM) is about identifying those parts of your business that you can't afford to lose – such as information, stock, premises, staff, services (e.g. electric, gas, water, telecommunications) – and planning how to maintain these if an incident occurs.

Any incident, large or small, whether it is natural, accidental or deliberate, can cause major disruption to your business or organisation. However, if you plan in advance, rather than waiting for it to happen, you will be able to get back to business in the quickest possible time. Delays could mean you lose valuable business to your competitors, your customers lose confidence in you, or in the worst case your business is no longer able to continue.

This affects you

Whether you are a market trader, a voluntary organisation, a Small Medium-Sized Enterprise (SME)[1] or a global institution you need to be able to continue with your critical activities, whatever happens.

You also need to make sure that your key suppliers and partners have their own effective Business Continuity Management arrangements in place, as an incident affecting them could significantly impact on your business or organisation.

Developing Business Continuity (BC) arrangements and documenting your procedures in a plan, will assist you in managing the risks that may affect your business or organisation to ensure that you can continue operating to a pre-determined minimum level. This will enable you to continue operating during and beyond an emergency.

Who is this advice for?

This advice is relevant to all business owners, managers and employees of SMEs as well as voluntary organisations.

This information will guide you through some planning steps that could help your business/organisation overcome a disruptive incident. The process doesn't have to take up vast resources. However, early planning can help prevent minor issues turning into more serious disruption for your business/organisation.

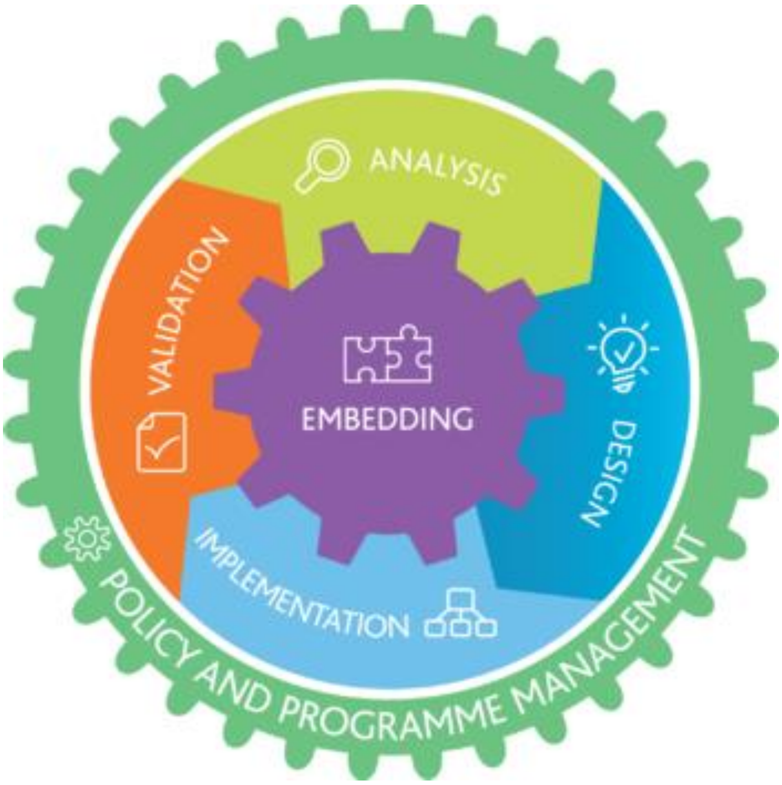
Once the basics of BCM have been understood, this document also refers to an example Business Continuity Plan template that you can adapt for your business/organisation – **A copy of the template can be found on your local authority's website.**

By following this step-by-step guide, applying BCM and completing a plan, your business/organisation will be better placed to deal with a disruption. This guide has been developed based on the latest BC international standards and process as promoted by the leading organisation in the field, the Business Continuity Institute (BCI).

[1] SME – Businesses whose personnel numbers fall below a certain limit, usually <250.

The Business Continuity Management (BCM) Lifecycle

This information aims to guide you through the steps you will need to take to implement BCM in your organisation. There are six Professional Practices (PP) that make up the BCM lifecycle as set out in the Business Continuity Management Standard (ISO 22301:2012, ISO 22313:2012 and the Business Continuity Institute's Good Practice Guidelines GPG 2018), and these are depicted in the diagram below.



Source: BCI Good Practice Guidelines 2018

By following this guide, you will be able to understand BCM and develop a Business Continuity Plan specific to your business/organisation. The six Professional Practices may have to be applied at different levels of detail depending on your business/organisation. These are:

- **PP1** ~ Policy and Programme Management
- **PP2** ~ Embedding
- **PP3** ~ Analysis
- **PP4** ~ Design
- **PP5** ~ Implementation
- **PP6** ~ Validation

PP1 ~ Policy and Programme Management

Effective programme management will ensure that BCM capability is established and maintained within your organisation.

Assigning responsibilities ~ It is essential that BCM has the support of senior management and it is suggested that an individual is nominated to be accountable for BCM across the business/organisation, supported by other colleagues as appropriate. Without this support, it will be virtually impossible to instill a sense of value and ownership among the rest of the workforce.

Establishing and implementing BCM in the organisation ~ One of the early tasks should be to agree the BCM policy for the organisation. This would normally be the responsibility of the management board representative, working with others as appropriate, and should set out:

- Scope, aim and objectives of BCM in the organisation; and
- The activities or "programme" that will be required to deliver these.

The policy should be owned by the management board and regularly reviewed.

Once the policy has been developed and agreed, it will be the task of the individual or team with responsibility for BCM to ensure the policy is implemented: This will involve:

- Communicating the programme to internal stakeholders;
- Arranging appropriate training for staff;
- Ensuring activities are completed, and
- Initial exercising of the organisation's BCM arrangements.

Ongoing Management ~ There are a number of activities that should be undertaken on an ongoing and relevant basis to ensure that BCM continues to be embedded in the organisation and remains current. These are:

- Making sure that the organisation's business continuity plans, and related documents, are regularly reviewed and updated (suggest time periods, monthly, yearly, etc.);
- Regular and frequent promotion of business continuity across the organisation;
- Administering the exercise programme; and
- Keeping the BCM plan updated through lessons learned and good practice.

PP2 ~ Embedding Business Continuity (BC)

Embedding Business Continuity is one of the ongoing activities resulting from the BCM Policy and Program management stage of the BCM Lifecycle. This Professional Practice continually seeks to integrate BC into day-to-day business activities and organisational culture – all business activity should be carried out with Business Continuity in mind. This can be achieved through any of the following:

- Developing a culture of Business Continuity awareness;
- Managing an awareness campaign and / or;
- Managing a training programme.

This activity is not unique to BC; other disciplines also need to be embedded in the organisation in a similar way. Disciplines such as Quality Assurance, Health and Safety, Environmental Services, Cyber Security and Risk Management have similar challenges. So, the opportunity to share experience and learning opportunities across various related disciplines is important.

PP3 ~ Analysis

Analysis is the Professional Practice within the BCM Lifecycle that reviews and assesses an organisation in terms of what its objectives are, how it functions and the constraints of the environment in which it operates.

The main technique used for the analysis of an organisation for Business Continuity (BC) purposes is the Business Impact Analysis (BIA). Completing a BIA and a Risk Assessment (RA) will enable you to better understand your business and priorities for recovery.

A secondary method used in the analysis of an organisation is known as “threat evaluation” which is used to estimate the likelihood and potential impact on specific activities from known threats. Threat evaluation is part of the wider methods used for risk assessment by organisations.

Business Impact Analysis (BIA) ~ A BIA identifies and documents your organisation’s key functions and services, what activities and resources are required to deliver these, and the impact that a disruption of these activities would have on your organisation.

You should complete a BIA for each of your key functions and services.

You will find an example format for a BIA in the Business Continuity Plan template. This will take you through the impact of a disruption over time and the resources you require to recover.

The information collected in each of your BIAs can be added into your Business Continuity Plan.

Risk Assessment (RA) ~ In relation to Business Continuity Management, the Risk Assessment looks at the likelihood and impact of a variety of risks that could cause business disruption.

You need to consider what risks could disrupt the key functions and services that you have identified within your BIA. These should include:

- Loss of staff;
- Loss of systems (ICT);
- Loss of utilities e.g. gas, water, electricity;
- Loss of, or access to premises;
- Loss of key suppliers / partners;
- Disruption to transport; and
- Other business specific risks.

While the above risks can be considered “generic” or “cross-cutting”, other risks will be specific to your business/organisation and should be addressed too. The Risk Assessment needs to be completed before you complete your plan, and solutions to these risks becoming realised need to be built in, to secure continuity of your activities.

PP4 ~ Design

This concerns a BCM strategies selection – following the collection of information from the business impact analysis (BIA) this stage allows the development of informed strategies to determine how continuity and recovery from disruption will be achieved. This stage also balances recovery priorities and costs. Recovery options should be considered at least for:

- People and accommodation – including alternative premises either owned, leased or through agreement with a third party;
- IT systems and networks – including recovery of IT systems, hardware, applications, software and networks, and the data used within these systems and facilities;
- Critical services such as utilities, and postal services;
- Critical assets such as paper records and reference material;
- Specialist business processes or services;
- Service provision by third party contractors.

The quicker an organisation aims to recover the critical activities (hence the shorter Recovery Time Objective - RTO), normally the more expensive the solution/strategy to recover or maintain these.

Strategies for dealing with one or more of the above situations could belong to one of these categories:

- Diversification – undertaking of activities from one or more locations;
- Replication – effectively copying resources in various locations;
- Standby – mothballing facilities;
- Post incident acquisition – acquiring resources required after an incident;
- Do nothing – waiting until the incident has occurred before deciding what to do. This is normally used in case of specialist equipment or skills difficult to obtain (note: the "do nothing" strategy is selected by default by all organisations that have not implemented Business Continuity);
- Subcontracting – use of third parties to undertake activities;
- Insurance – can provide compensation, but unlikely to cover full impacts of an incident. It is recommended that insurance is scrutinised very carefully;
- Reliability – use tried and tested equipment, processes, and third parties of the highest reputation.

PP5 ~ Implementation

Plan development – documents the agreed strategies and tactics thorough the process of developing a working Business Continuity Plan. A plan should be:

- Direct – should provide clear, action orientated direction;
- Adaptable – enabling response to a wide range of incidents, including not only anticipated ones;
- Concise – should only contain guidance, information and tools to be used in an incident.
- Relevant – the information should be current and applicable.

The BCP should dovetail with other relevant plans e.g. Information Technology Disaster Recovery Plan, Emergency Response Plan, Evacuation Plan, etc. It should be easily accessible, current and provided to all members of staff. A useful tip is to create a single page "aide memoire" or "action card" for each team and each critical activity identified, that can be accessed at all times. Other considerations at this stage are the establishment and implementation of staff rotas, a robust crisis management structure, activation and mobilisation, meeting venues, communications, and a procedure for standing down. It is important that the plan benefits from management input, consultation, review and sign off.

The key requirements for an effective response by the organisation are:

- The ability to recognize and assess existing and potential threats when they occur and to determine an appropriate response;
- A clear and understood procedure for the activation, escalation and control of the organisation’s incident response procedures (the incident response structure);
- Having responsible personnel with the authority and capability to implement the agreed-upon continuity strategies (or objectives) as defined within the organisation’s plans to continue and recover the disrupted activities;
- An ability to communicate effectively with internal and external interested parties; and
- Access to sufficient resources to support the BC strategy.

The outcomes can be achieved by various methods and techniques and, whatever approach is adopted, it is important that it is suitable for the needs of the organisation.

The table below provides some of the strategies that you could adopt to protect your resources and critical activities. This list is not exhaustive.

People

- Inventory of staff skills not utilised within their existing roles ~ to enable redeployment.
- Process mapping and documentation ~ to allow staff to undertake roles with which they are unfamiliar.
- Multi-skill training of each individual.
- Cross training of skills across a number of individuals.
- Succession planning.
- Use of third-party support, backed by contractual agreements.
- Geographical separation of individuals or groups with core skills can reduce the likelihood of losing all those capable of undertaking a specific role.

Premises

- Relocation of staff to other accommodation owned by your organisation such as training facilities.
- Displacement of staff performing less urgent business processes with staff performing a higher priority activity. Care must be taken when using this option so that backlogs of less urgent work do not become unmanageable.
- Remote working ~ this can be working from home or other locations.
- Use premises provided by other organisations, including those provided by third party specialists.
- Alternative sources of plant, machinery and other equipment.

Technology

- Maintaining the same technology at different locations that will not be affected by the same business disruption.
- Holding older equipment as emergency replacement or spares.

Information

- Ensure data is backed-up and it is kept off site.
- Essential documentation is stored securely (e.g. fireproof safe).
- Copies of essential documentation are kept elsewhere (electronic and hard copies).

Suppliers and Partners

- Storage of additional supplies at another location.
- Dual or multi-sourcing of materials.
- Identification of alternative suppliers.
- Encouraging or requiring suppliers / partners to have a validated business continuity capability.
- Significant penalty clauses on supply contracts for failure to supply.

Stakeholders

- Mechanisms in place to provide information to stakeholders.
- Arrangement to ensure vulnerable groups are accommodated.

PP6 ~ Validation

The purpose of Validation is to ensure that the BC capability reflects the nature, scale and complexity of the organisation it supports and that it is current, accurate, and complete, and that actions are taken to continually improve organisational resilience.

BCM arrangements cannot be considered reliable until they have been exercised and have proved to be workable. Exercising should involve validating plans, rehearsing key staff and testing systems which are relied upon to deliver resilience. The frequency of exercises will depend on your business/organisation but should consider the rate of change (to the organisation or its risk profile), and outcomes of previous exercises (if particular weaknesses have been identified and changes made). As a minimum, it is suggested plans are exercised annually.

Validation is the stage in the BCM life cycle confirming that the BCM Programme meets the objectives set in the policy and that the BCP is fit for purpose. Establishing an exercise programme is vital for ensuring that all staff are made aware of the implications of Business Continuity and their roles and responsibilities in a BC situation.

There are a number of different mechanisms that can be utilised to support the organisation and awareness process, including:

- Incorporating BCM information into the staff induction process;
- Disseminating information via the intranet, newsletters, e-mails and bulletins to raise awareness;
- Talking about BCM at team meetings;
- Using standard procedures such as fire drills to discuss the various incident procedures;
- Running seminars or workshops to exchange information and explore roles and responsibilities;
- Including BCM as a standing agenda item at senior management team meetings.

A regular programme of testing and exercising is also required to ensure the plan is viable and reflects the most up to date changes. Exercising the plan is the only means to ensure that all procedures, strategies, contacts, communication lines etc. identified in the plan will work and are up to date.

The frequency, type and depth of testing and exercising will depend on a variety of factors such as:

- Size of the business/organisation – the larger the size, the more comprehensive the exercise needs to be;
- Criticality of the activities/services – the higher the criticality, the higher the exercising frequency;
- The specifics of the activity/service – there are some activities/services that can only be tested live;
- Cost efficiencies – if there are cost benefits to holding tests as a group of services, these should be considered;
- The rate of change of the organisation/business – the more alert the change, the higher the required exercising frequency.

Exercises should be followed by a debriefing session which should capture all the lessons identified and associated actions in a post exercise report. An action plan should be developed and monitored by those responsible for BCM and who ensure that implementation takes place. Debriefs can be undertaken using a systematic approach and it is suggested that persons be trained if possible, on how to effectively undertake/chair a debrief process.

Validation could be achieved through the following three activities:

- Exercising;
  - **Testing ~** Not all aspects of your plan can be tested but some elements can, such as contact lists and activation process. You can also test back up power, communications equipment and Information Communication Technology (ICT) back-ups.
  - **Discussion based exercises ~** This involves bringing people together to discuss the plan and their individual responsibilities. It is useful for training purposes and for validation of a new plan.
  - **Table-Top Exercise (TTX) ~** This is an efficient method of validating plans and rehearsing key staff. Staff are brought together to take decisions on their actions as a scenario unfolds. To run this type of exercise you need to develop a scenario and set questions for the participants to consider.
  - **Live exercise ~** This can range from a small-scale test of one component, such as evacuation, through to a full-scale test of many components of the plan. Before running a large-scale live exercise, you must consider if your organisation has the capacity to run it without causing a disruption to your ability to deliver your key functions and services.
- Auditing is essential to provide the organisation/business with the assurance that the BCM process is working, and demonstrating continuous improvement where considered necessary.
- Maintenance: -
  - Lessons learned through exercising.
  - Changing in organisational structures, products and services, infrastructure, processes or activities.
  - Review or audit.
  - A real incident, where lessons learned can be incorporated.
  - Changes or updates in the business continuity management lifecycle, such as the BIA or continuity solutions.

- Review: -
    - Audit.
    - Self-assessment.
    - Quality assurance.
    - Performance appraisal.
    - Supplier performance.
    - Management review.

Preparing an Emergency Kit

To assist you in your response you can develop an Emergency Kit in advance. An Emergency Kit contains items that will help you implement your plans. Your pack should be stored safely and securely off-site. Ensure that the pack is checked and updated regularly.

Examples of items to go in an Emergency Kit include:

Documents

- Business Continuity Plan ~ your plan to continue and to recover your business
- List of employees with contact details and next of kin
- Contact details of customers and suppliers
- Contact details for emergency glaziers, salvage organisations and building contractors
- Contact details for utility companies (electricity, gas, water and telecommunications)
- Building site plan / floor plan including location of gas, electricity and water shut off points
- Insurance, finance and banking details

Equipment

- Computer back up tapes / disks / USB memory sticks or flash drive (consider security of these if placed in your emergency pack)
- Spare keys / security codes
- Torch and spare batteries
- Hazard and cordon tape
- Message pads
- General stationery
- Disposable camera (useful for recording evidence in an insurance claim)
- Cash
- Wind up radio
- Mobile telephone charger

This guidance is provided as general information about Business Continuity Management and planning for emergencies. It is not intended to replace detailed guidance and planning specific to you and your organisation. You should consider whether you need to obtain this. To the extent permitted by law, Dorset Local Resilience Forum (Dorset LRF), Dorset Council and Bournemouth, Christchurch and Poole Council exclude any liability arising from the use of this document and example template.

It is important to ensure that your plans are easily accessible, and copies should be kept on and off site, but secure and compliant with the Data Protection Act 2018.

This guide has been developed by Dorset Council and Bournemouth, Christchurch and Poole Council, with support from the Dorset Local Resilience Forum.

For additional information, advice or guidance about BCM please contact your local authority. The list below has the contacts for Dorset.

Local Authority – Emergency Planning / Business Continuity Teams

Dorset Council		
01305 251000	emergencyplanningteama@dorsetcouncil.gov.uk	www.dorsetcouncil.gov.uk
Bournemouth, Christchurch & Poole Council		
01202 451451	emergency.planning@bcpcouncil.gov.uk	www.bcpcouncil.gov.uk
Dorset Civil Contingencies Unit – Dorset Local Resilience Forum		
01202 229044	ccuadmin@dwfire.org.uk	www.dorsetprepared.org.uk