CabinetOffice

Chapter 6 Business Continuity Management

Revision to *Emergency Preparedness*

Chapter 6 (Business Continuity Management) of *Emergency Preparedness*, Revised Version

Summary

- The Act requires Category 1 responders to maintain plans to ensure that they can continue to exercise their functions in the event of an emergency so far as is reasonably practicable. The duty relates to all functions, not just their emergency response functions (*paragraphs 6.1 – 6.13*).

- Category 1 responders must have regard to assessments of both internal and external risks when developing and reviewing business continuity plans (BCPs) (*paragraphs 6.14 - 6.16*).

- Business continuity plans may take the form of generic plans - which set out the core of a Category 1 responder's response to any BCM event - or specific plans dealing with particular risks, sites or services (*paragraphs 6.17 - 6.19*).

- There must be a clear procedure for invoking the business continuity plan (*paragraphs 6.20*).

- BCPs must include arrangements for exercises for the purpose of ensuring the plan is effective, and arrangements for the provision of training to those involved in implementing the plan. Plans must be reviewed and kept up to date (*paragraphs 6.21 - 6.28*).

- Category 1 responders are required to publish aspects of their BCPs insofar as making this information available is necessary or desirable for the purposes of dealing with emergencies (*paragraph 6.29 - 6.31*).

- The British Standard for Business Continuity (BS25999) is widely acknowledged as industry best practice. It provides a generic framework that is applicable across the public, private and voluntary sectors. (*paragraphs 6.43 - 6.107*).

WHAT THE ACT AND THE REGULATIONS REQUIRE

Scope of the duty

6.1.   The Act requires Category 1 responders to maintain plans to ensure that they can continue to perform their functions in the event of an emergency, so far as is reasonably practicable.[1]

6.2.   The duty to maintain plans relates to all the functions of a Category 1 responder, not just its civil protection functions. For Category 1 responders to help others in the event of an emergency, they first need to be able to keep their own crisis response capabilities going. However, Category 1 responders also need to be able to continue to deliver critical aspects of their day-to-day functions (e.g. law enforcement, looking after vulnerable people, attending minor fires) in the event of an emergency, if the impact on the community is to be kept to a minimum.

---

[1] s.2(1)(c)

6.3.   It may, therefore, be helpful to think of the business continuity management (BCM) duty in the Act as being separated into two strands. In practice, the Act requires Category 1 responders to maintain plans to ensure that they can:

> o   continue to exercise their civil protection functions: The legislation requires Category 1 responders to maintain plans to deal with emergencies (see Chapter 5) and put in place arrangements to warn and inform the public in the event of an emergency (see Chapter 7). The BCM duty requires Category 1 responders to maintain plans to ensure that they can deliver these capabilities when they are required.

> o   continue to perform their ordinary functions: Category 1 responders perform a range of functions that are important to the human welfare and security of the community and its environment (e.g. provision of health care, detection of crime, fighting fires). This is particularly true in an emergency situation, where operational demands often increase and the operating environment can become more challenging. The legislation requires Category 1 responders to make provision for ensuring that their ordinary functions can be continued to the extent required.

6.4.   Organisations should not only look at the resilience of internal structures and processes, but also those of organisations they rely on, or deliver services through.

6.5.   The Act requires Category 1 responders to put in place plans to ensure that they can continue their functions in the event of an emergency.[2] This requires them to ensure that those organisations delivering services on their behalf (e.g. contracted-out services) or capabilities which underpin service provision (e.g. information technology and telecommunications providers) can deliver to the extent required in the event of an emergency. This is because services remain part

[2] s.2(1)(c)

of an organisation's functions even if they do not directly provide them.

Limits of the duty

Definition of emergency

6.6.	BCM is a flexible framework designed to help organisations to continue operating in the face of a wide range of different types of disruptions right the way along the spectrum of severity. BCM does not however embrace all dimensions of an organisation's resilience, and one important distinction is between BCM and crisis management. The Publicly Available Specification on Crisis Management (PAS200) identifies crisis management as wider ranging and inherently strategic in nature. BCM in turn is a more operationally-focused activity to ensure that service disruptions are managed, potentially cascading impacts are mitigated and services are maintained. For further details and for guidance on developing a crisis management capability see http://epcollege.com/epc/news/pas200-crisis-management---new-guidance-for-crisis/ (including link to the BSI website).

6.7.	The BCM duty, however, is determined by the definition of emergency in the Act. The Act therefore imposes a duty on Category 1 responders to put in place plans to ensure that they can continue to exercise their functions in the event of a much narrower range of disruptive challenges.[3]

6.8.	The duty applies only to those events or situations defined as an emergency in section 1 of the Act - events or situations that threaten serious damage to the human welfare, environment or security of a place in the United Kingdom. This should be read in conjunction with section 2(2) of the Act, which provides that an event or situation is only an emergency when it overwhelms existing response arrangements, and cannot be dealt with within existing resources or procedures (see Chapter 1 for an in-depth description of the definition of "emergency" underpinning Part 1 of the Act).

[3] s.2(1)(c) and s.2(2)

6.9.   While the duty focuses on the most challenging situations, it is likely that plans put in place to fulfil their duty under the Act will help Category 1 responders to prepare for a much wider range of day-to-day (i.e. non-emergency) interruptions. By putting in place plans to keep themselves going in the event of an emergency, Category 1 responders will build resilience to a wider range of less serious events.

Practicability

6.10.   Ideally, Category 1 responders would be able to continue all of their functions at ordinary service levels in the event of an emergency. In practice, this may not prove possible, and therefore the duty is qualified.

6.11.   The Act requires Category 1 responders to put in place arrangements to ensure that they continue to exercise their functions in the event of an emergency so far as is reasonably practicable.[4]

6.12.   The qualification "so far as is reasonably practicable" has three elements to it:

   o   **Criticality:** Category 1 responders should focus on ensuring that they can deliver critical functions. Which of its functions are critical is a matter that can be determined only by the organisation itself, and may depend on the nature of the emergency in question. Category 1 responders should not lose sight of the common supporting infrastructure underpinning these functions. The following guiding principles should be used when deciding whether or not a service or activity is critical. It is not intended to be a definitive list, but rather a series of useful indicators:

[4] s.2(1)(c)

- **Emergency management/civil protection:** Functions that underpin the Category 1 responder's capability to respond to the emergency itself, and take effective action to reduce, control or mitigate the effects of the emergency.

- **Impact on human welfare, the environment and security:** The significance of services to the effective functioning of the community in the event of an emergency, or an adverse effect on the environment.

- **Legal implications:** Statutory requirements on Category 1 responders and the threat of litigation if a service is not delivered, or is delivered inadequately.

- **Financial implications:** Loss of revenue and payment of compensation.

- **Reputation:** Functions that impact on the credibility and public perception of a Category 1 responder.

o **Service levels:** The Act does not require Category 1 responders to continue to deliver their functions at ordinary levels in the event of an emergency. Some critical functions may need to be scaled up, while others (which are non-critical) may need to be scaled down or suspended. Acceptable levels of service in the event of an emergency are a matter for the Category 1 responder itself to determine in the light of its capabilities, constraints and the needs of the community.

o **Balance of investments:** No organisation will be in a position to commit unlimited resources to BCM. It is the role of the Category 1 responder itself to decide the level of protection sought.

6.13.   Category 1 responders must therefore put in place a process for effectively managing the prioritisation of services - and getting high-level endorsement for these decisions - prior to an emergency occurring. The business impact analysis (BIA) process described later in this chapter gives a methodology for undertaking this work.

Risk assessment

6.14.   It is important that Category 1 responders identify the significant risks threatening the performance of critical functions in the event of an emergency or disruption, as this will enable them to focus resources in the right areas, and develop appropriate continuity strategies.[5]

6.15.   In this context, there are two strands to risk assessment, relating to external threats (i.e. risk of an emergency occurring) and internal risks (i.e. business risks) that could cause loss or disruption of critical services required to control, reduce or mitigate the effects of an emergency or disruption.

6.16.   The Act requires Category 1 responders to identify and assess significant risks of an emergency occurring in their area[6] - in accordance with their particular functions - as a basis for performing their other civil protection duties (see Chapter 4). The Regulations require Category 1 responders to have regard to assessments of risk maintained pursuant to the Act when developing BCPs.[7] The Act requires Category 1 responders to consider whether a risk assessment makes it necessary or desirable to review a BCP.[8] It is good practice, in any instance, to review BCPs in conjunction with risk registers and vice versa.

---

[5] regulation 21
[6] s.2(1)(a)
[7] regulation 19
[8] s.2(1)(e)

Generic and specific plans

6.17. As with emergency plans, the Regulations provide that Category 1 responders may use generic plans, specific plans, or a combination of the two in business continuity planning. A generic plan is a core plan which enables a Category 1 responder to respond to a wide range of possible impacts, setting out the common elements of the response to these (e.g. invocation procedure, command and control, access to financial resources).

6.18. Specific plans may be required in relation to specific risks, sites or services. Specific plans provide a detailed set of arrangements designed to go beyond the generic arrangements when these are unlikely to prove sufficient.

6.19. Specific plans will usually operate within the framework established by the generic plan. It is a matter for Category 1 responders themselves to decide - in the light of assessments of risk - what, if any, specific plans are required.

Plan invocation

6.20. The Regulations specifically require Category 1 responders to establish a procedure for determining when an emergency has occurred which affects its ability to continue to perform its functions.[9] In other words, there must be a clear procedure for invoking the plan. Where continuity of critical functions is threatened in the event of an emergency, there should be a clearly laid out escalation procedure. This should be identified, agreed and documented within the plan. The Regulations specifically require this procedure to:

---

[9] regulation 24

- o   identify the person who should determine whether such an emergency has occurred;

- o   specify the procedure that person should adopt in taking that decision;

- o   specify the persons who should be consulted before such a decision is taken; and

- o   specify the persons who should be informed once a decision has been taken.

Exercising BCPs

6.21.   Exercises provide demonstrable evidence of a business continuity and incident management competence and capability. A BCP cannot be considered reliable until it is exercised and has proved to be workable. As part of the BC process there is a continual need to prove plans and strategies by testing. No matter how well designed and thought-out a BCM strategy or BCP appears to be, a series of robust and realistic exercises will identify areas that require amendment.

6.22.   The Regulations require Category 1 responders to put in place arrangements for exercising BCPs in order to ensure that they are effective.[10] These arrangements should encompass the three principal purposes of exercising:

- o   **validating plans** - to verify that the plan works;

- o   **rehearsing key staff** - to familiarise key staff with what is expected of them in a crisis and preparing them for crisis conditions; and

- o   **testing systems** - to ensure that systems relied upon to deliver resilience (e.g. uninterrupted power supply) function correctly and offer the degree of protection expected.

[10] regulation 25(a)

6.23.   As a simple rule, if it has not been tested it does not work. Exercising must be maintained to hold credibility and encourage ownership across the organisation. Tests should build on the organisation's past experience. The exercising programme should be flexible, and the focus and frequency of exercises should be responsive to:

- o **the rate of change** - where the pace of change (e.g. to the organisation or risk profile) is particularly rapid, exercises may need to be more frequent; and

- o **outcomes of previous exercises** - the identification of particular weaknesses and subsequent changes to plans may necessitate further exercising.

Training key staff

6.24.   It is important to ensure that relevant people across the Category 1 responder - and in other organisations where appropriate - are confident and competent concerning the plan. It is particularly important that staff receive appropriate training prior to exercising. This will ensure that they are adequately prepared for what can be a challenging experience.

6.25.   The Regulations require Category 1 responders to put in place a training programme for those directly involved in the execution of the BCP should it be invoked.[11] This should be reflected in plans. This should cover:

- o **the contents of the plan** - how is the plan invoked? What are the key decision-making processes? Who else needs to be involved?

[11] regulation 25(b)

> o **their role in implementing the plan** - what is expected of them? How do they fit into the wider picture?
>
> o **key skills and knowledge required in crisis response.**

Reviewing and maintaining BCPs

6.26. The Act specifically requires Category 1 responders to maintain business continuity plans to ensure that they can continue to deliver key services in the event of an emergency.[12] This means that Category 1 responders must not only put plans in place, but ensure that they are reviewed and kept up to date.

6.27. Category 1 responders exist in a dynamic environment - organisations themselves and the environment they operate in are subject to change. BCPs need to be reviewed and updated to ensure that they remain valid. The following aspects of plans should be reviewed:

> o **personnel** - staff turnover means that contact details will need constant updating;
>
> o **the responsibilities of the Category 1 responder** - where a Category 1 responder takes on new functions or delivers new services, this should be reflected;
>
> o **organisational structures** - where responders have experienced restructuring this may need to be reflected in plans;
>
> o **suppliers or contractors** - ensuring that the details of suppliers and contractors are kept up to date;
>
> o **risk assessments** - the Act requires Category 1 responders to review plans in the light of changes to risk assessments;[13] and
>
> o **business objectives/processes.**

---

[12] s.2(1)(c)
[13] s.2(1)(e)

6.28.   The frequency of plan review will depend on the rate of change within the organisation and the environment it operates within. Plan maintenance should take place on an ongoing basis, but all business continuity plans should be comprehensively reviewed at appropriate intervals.

Publication of BCPs

6.29.   Communication with customers or service users - who may need information about service continuity in the event of an emergency - is important to community resilience. Emergencies cause serious disruption to people's lives and increase reliance on public sector bodies - provision of information about what they can and cannot expect from Category 1 responders in the event of an emergency, may help to minimise this disruption.

6.30.   The Act requires the publication of aspects of BCM plans in so far as this is necessary or desirable for the purposes of preventing, controlling or mitigating the effects of an emergency or otherwise responding to the emergency.[14]

6.31.   Category 1 responders need only publish information where there is a positive benefit in doing so. For example, a Category 1 responder need not publish internal management information which would be of little relevance or interest to the public. Furthermore, the Regulations prohibit the publication of sensitive information (e.g. commercially confidential information, personal data) where consent has not been received from the originator of the information, or where the public interest in disclosure fails to outweigh the interests of the organisation or individual concerned.

---

[14] s.2(1)(f)

Box 6.0: Further advice and information

Also included in this chapter is further advice about BCM and information that is not supported directly by the Act, but responders may find it useful in fulfilling their duties under the Act. These sections of text are distinguished by inclusion in a text box like this one.

How the Act and Regulations apply in Scotland, Wales and Northern Ireland

6.32.   The Act and the Regulations apply in Scotland to bodies outside devolved competence in the same way as they apply in England.

6.33.   The Regulations made by the Scottish Ministers make provision as to how Category 1 responders in Scotland that fall within devolved competence, should exercise their duty under the Act to maintain business continuity plans.

Wales

6.34.   The Act and the Regulations apply in Wales in the same way as they apply in England.

Northern Ireland

6.35.   The Act and the Regulations apply to Category 1 responders exercising functions in Northern Ireland in the same way as they apply in England, but see information in Chapter 12 in relation to the Police Service of Northern Ireland.

HOW THE REQUIREMENTS OF THE ACT AND THE REGULATIONS MAY BE CARRIED OUT

6.36. This section provides practical guidance on taking forward a BCM programme within a Category 1 responder organisation. It describes the discipline of BCM and outlines a methodology for implementing it. Category 1 responders must have regard to this material and may find it useful in fulfilling their duties under the Act. While the Government considers this to be a sound approach, Category 1 responders may use other models to deliver statutory requirements where there are compelling reasons for doing so.

6.37. The Government is keen to give Category 1 responders the flexibility to make the best use of the resources and expertise available to them. The Regulations permit Category 1 responders to enter into collaborative arrangements in order to fulfil the BCM duty.[15] Category 1 responders may:

- o   deliver the duty separately;
- o   deliver the duty jointly (e.g. by forming a joint BCM unit or resource);
- o   agree that one Category 1 responder will facilitate the delivery of a BCM programme on behalf of a number of other Category 1 responders; or
- o   enter into collaborative arrangements in which one or more Category 1 responder gives assistance to others in fulfilling their BCM duties (e.g. managing the overarching programme, developing framework plans).

[15] regulations 8 and 9

6.38.   However, BCM must be owned and driven within the organisation itself - and engage the expertise and resources of its staff - in order to be effective. While collaborative arrangements can be used to make use of BCM expertise or resources in other Category 1 responders, responsibility for the robustness of BCM arrangements must remain within the organisation.

What is business continuity and business continuity management?

6.39.   Business continuity [16] is the strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level.

6.40.   Business continuity management provides the strategic framework for improving an organisation's resilience to interruption. Its purpose is to facilitate the recovery of key business systems and processes within agreed time frames, while maintaining the delivery of the Category 1 responder's identified critical functions. It assists organisations to anticipate, prepare for, prevent, respond to and recover from disruptions, whatever their source and whatever aspect of the business they affect.

6.41.   BCM is a holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause. It also provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and core business activities. Business continuity management involves managing the recovery or continuation of activities in the event of a disruption, and management of the overall programme through training, exercises and reviews, to ensure business continuity plans stay current and up-to-date.
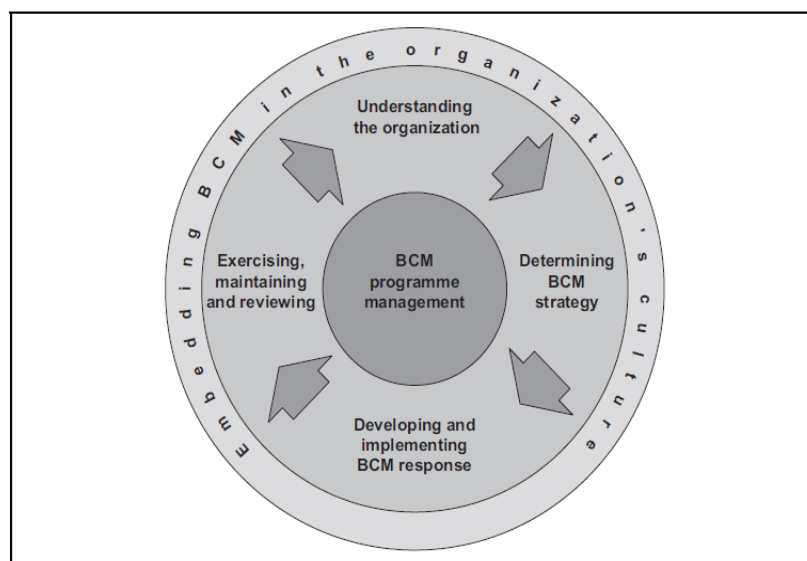
[16] BS25999 definition of business continuity

6.42.　BCM is valid across the public, private and voluntary sectors. It is about maintaining the essential business deliverables of an organisation in an emergency. The primary 'business' of private sector organisations is the generation of profit, a process that BCM seeks to protect. Category 1 responders provide services to the public, and it is equally important that these are protected and resilient.

BCM methodology

6.43.　The British Standard for business continuity (BS25999) works on a six-stage process widely acknowledged as best practice. This model provides a generic framework that is applicable across the public, private and voluntary sectors. This standard, or its equivalent in the water industry, the Security and Emergency Measures Direction (SEMD), provide a good basis for BCM.

6.44.　Figure 6.1 illustrates this approach. The rest of the chapter describes this process, and supports Category 1 responders in using this framework to fulfil their duties under the Act.

Figure 6.1: The business continuity management lifecycle

BS 25999-1:2006 BRITISH STANDARD business continuity management Part 1: Code of Practice [17]

[17] Permission to reproduce extracts from BS25999 is granted by BSI. British Standards can be obtained in PDF or hard copy formats from the BSI online shop: www.bsigroup.com/Shop or by contacting BSI Customer Services for hardcopies only: Tel: +44 (0)20 8996 9001, Email: cservices@bsigroup.com.

6.45.   As Figure 6.1 shows, the six stages of the process are:

- o **Stage 1: BCM programme management:** Programme management is at the heart of the process. It requires the participation of senior management and establishes the organisation's approach to business continuity.

- o **Stage 2: Understanding the organisation:** This element assists in the understanding of the organisation through the identification of its key products and services and the critical activities and resources that support them. This element ensures that the BCM programme is aligned to the organisation's objectives, obligations and statutory duties.

- o **Stage 3:** Determining business continuity strategy: This element allows the organisation to select its strategies in order to meet its objectives.

- o **Stage 4:** Developing and implementing a BCM response: This stage looks at the need for Category 1 responders to develop and implement plans and arrangements to ensure continuity of critical activities, and the management of an incident.

- o **Stage 5:** Exercising, maintaining and reviewing BCM arrangements: An organisation's arrangements cannot be considered reliable until exercised. This element ensures that an organisation's BCM arrangements are validated by exercise and review and that they are kept up-to-date.

- o **Stage 6:** Embedding BCM in the organisation's culture: Business continuity must become part of the way an organisation is managed to be effective. This stage provides the overarching element that ensures that opportunities are used at the various stages of the BCM process.

Delivering BCM arrangements

Stage 1: BCM programme management

6.46.   In order to be successful, BCM must be regarded as an integral part of a Category 1 responder's normal management processes.

6.47.   Achieving top-level buy-in is vital to developing robust BCM arrangements. Engaging senior officers is crucial to the success of any major programme because of the influence they have over resource allocation and the culture of an organisation. However, the commitment of the top level is particularly important in relation to BCM because:

- o   it requires the leverage they exert across the organisation in order to be effective;
- o   it requires decisions about attitudes to risk and service prioritisation that can only be taken at the top level; and
- o   the top team is responsible for ensuring that effective governance arrangements are in place.

Leadership

6.48.   Experience has shown that there is merit in giving a member of the executive management board overall responsibility for the BCM process by being appointed as the champion within the organisation. This will ensure that the profile of BCM issues is increased and decisions are made at the appropriate level.

6.49.   BCM is an ongoing process and it is important to gain the support and endorsement of the board at the end of each stage of the cycle. Critically, it should be the responsibility of senior management to provide the assurance that BCM arrangements are robust and meet the requirements of the Act.

BCM co-ordinator

6.50.   Governance is about accountability, responsibility and control. A person with the appropriate seniority and authority should be identified as accountable for BCM policy, implementation and operation.

6.51.   Implementation planning should include arranging appropriate training for staff and exercising the capability; this stage is best carried out using a project management method to ensure that the implementation is effectively managed.

6.52.   Ongoing management of your BCM arrangements will contribute to business continuity becoming embedded within the organisation. Regular review, exercise and updating plans will ensure this happens. A review must take place of arrangements after change in the organisation; such as operating procedures, environment personnel, technology, and after an incident or exercise. If the change is significant to the organisation then a review of the Business Impact Analysis is also advised.

Stage 2: Understanding the organisation

6.53.   An accurate assessment of the Category 1 responder's organisation and its business is critical, as it will provide the basis upon which all subsequent BCM policies and processes are based.

6.54.   An understanding of the organisation comes from:

- o   the organisation's objectives, obligations, statutory duties and operating environment;

- o   the activities, assets and resources that support the delivery of key products and services;

- o   assessing the impact and consequences of failure of these activities; and

- o   identifying and evaluating the threats that could disrupt these.

6.55.   Category 1 responders should carry out a business impact analysis that assesses over time the impacts if the activity was disrupted; and establish the maximum tolerable period of disruption (MTPD) of each. MTPDs can be worked out by looking at the:

- o   time period after disruption that the activity must be resumed;

- o   minimum level needed upon resumption; and

- o   time period for achieving normal levels of operation.

Key to this is identifying interdependencies (assets, infrastructure, and resources) to be maintained.

6.56.   Category 1 responders should consider the following when assessing impacts:

- o   the impact on staff or public wellbeing;

- o   the impact of damage to, or loss of, premises, technology or information;

- o   the impact of breaches of statutory duties or regulatory requirements;

- o   reputation damage;

- o   damage to financial viability;

- o   deterioration of product or service quality; environmental damage; and

- o   external services and suppliers.

Category 1 responders should document this process (approach, findings and conclusions).

6.57.   Identification of critical activities is essential to prioritise the areas that need to be focused on. In basic terms, an organisation's critical activities are those that would have the greatest impact in the shortest time.

6.58.   Risk assessment is vital in evaluating threats, and risk should be understood in respect of the organisation's critical activities. By utilising recognised risk techniques, a scoring can be achieved. Guidance on conducting risk assessments can be found in Chapter 4 of this guidance. Annex 4F sets out a risk matrix that can be used to score impacts.

6.59.   Having identified those areas where the Category 1 responder is most at risk, a decision has to be made as to what approach is to be taken to protect the operation. This decision along with a documented list of key products and services, the business impact analysis and the risk assessment should be signed off by top management to ensure that the work is a true reflection of the organisation.

6.60.   As Annex 4F explains, the nature of the risk - defined in terms of its likelihood and impact - will determine which business continuity strategy is appropriate and what, if any, action is required. At one end of the spectrum, disruptions that are low likelihood and low impact may require no specific action, and may merely be dealt with through generic arrangements. Risks that are high impact and high probability, on the other hand, may point to the development of specific plans and risk mitigation strategies.

6.61.   A number of the strategies that could be adopted are given below:

- o   **do nothing** - in some instances top-level management may consider the risk to be acceptable;

- o   **change, transfer or end the process** - such decisions to alter business process must be taken with regard to the organisation's key objectives and statutory responsibilities;

- o   **insure** - may provide some financial recompense or support but will not aid the organisation's response and will not meet all losses (e.g. reputation and other non-financial impacts, human consequences);

- o   **mitigate loss** - tangible procedures to eliminate or reduce risk within the business; and

- o   **plan for business continuity** - an approach that seeks to improve the Category 1 and 2 responders' resilience to interruption, allowing for the recovery of key business and systems processes within the recovery time frame objective, while maintaining their critical functions.

6.62.   Any strategy must recognise the internal and external dependencies of the organisation and must have general acceptance by the management functions involved. The continuity strategies adopted here will shape the ability of a Category 1 responder to perform its critical functions in the event of an emergency, and it is important that these decisions are taken by the appropriate officers in the full light of the facts.

6.63.   The Act requires Category 1 responders to assess the risk of emergencies occurring ("emergency risk assessment") and use these assessments to inform emergency planning and business continuity planning (see Chapter 4).[18] The development of community risk registers will mean that Category 1 responders have access to up-to-date information about risks in their area. Contingencies that seriously disrupt the activities of the community may also limit the ability to respond to them effectively.

Stage 3: Determining business continuity strategy

6.64.   Category 1 responders should look at strategic options for its critical activities, while bearing in mind the most appropriate strategy will depend on factors such as: the maximum tolerable period of disruption, cost, and consequences of inaction.

6.65.   Strategies should be considered for the following areas:

- o **people -** e.g. multi-skill training; separation of core skills; use of third parties; succession planning; and knowledge retention and management;

- o **premises -** e.g. alternative premises/locations; working from home and remote sites;

- o **technology -** e.g. geographical spread; holding emergency

[18] s.2(1)(a),(b) and (e)

replacement, such as old equipment and spares, additional risk

mitigation for unique or long lead-time equipment; remote access;

third-party;

- o **information -** e.g. confidentiality; integrity; availability; and currency;

- o **supplies -** e.g.: storage of contingency stock at additional

  location; third part arrangements; assessing the BC capability of your

  suppliers; dual sourcing and; contractual and service level

  agreements; and

- o **stakeholders -** e.g. protect the interests of key suppliers and

  good relationship management.

6.66. Senior managers should sign off documented strategies.

Stage 4: Developing and implementing a BCM response

6.67. Business continuity planning is at the heart of the BCM process. The business continuity plans provide the framework in which the Category 1 responder mobilises its response to a BCM challenge in the event of an emergency. Plans normally consist of an Incident Management Plan, a Business Continuity Plan and a Business Recovery Plan.

6.68. In developing all plans, consideration should be given to:

- o **keeping it short, simple and user-friendly** - it will need to be

  read and understood in challenging and pressured circumstances;

- o **ensuring the assumptions contained are realistic** – e.g. numbers of

  staff directly affected by the incident, the effect of the 'backlog trap'

  (i.e. the impact of the accumulation of tasks left uncompleted

  on recovery);

- o **references to other sources of information and supporting documentation** – e.g. guidance, databases, lists of key contacts, resources and suppliers;

- o **action plans and checklists –** what should be provided

- o **ownership of key tasks -** these should be reflected in job descriptions;

- o **pro-formas** - giving templates and model documentation;

- o **version control** - the need to implement document management procedures, including a list of all plan holders, which has to be maintained, together with a distribution and change control process; and

- o **communications** - effective communication with stakeholders and, where appropriate, the media is crucial to an effective response
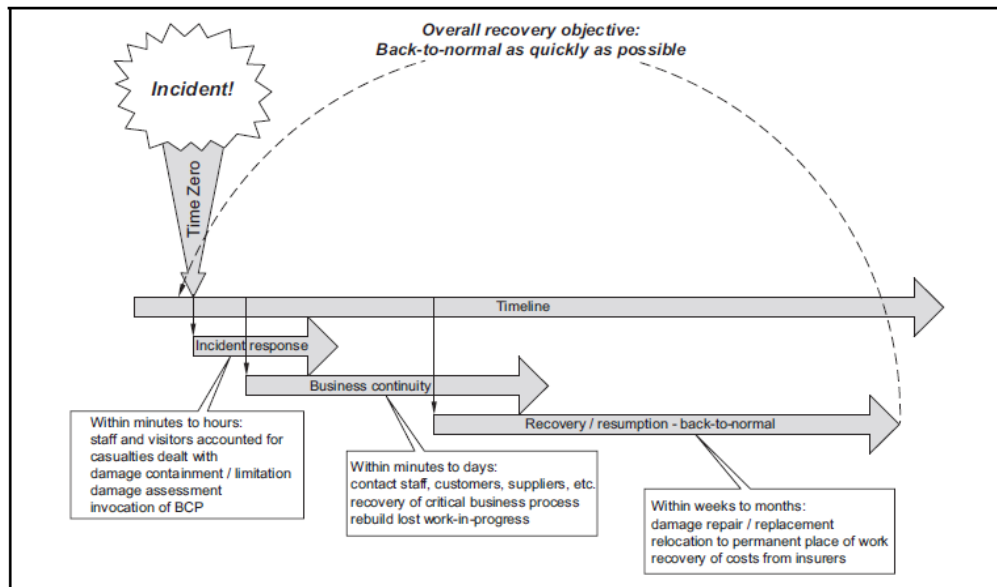
6.69. The structure, content and detail of the BCPs will depend on the nature of the Category 1 responder, the risk and the environment in which it operates. In particularly large or complex organisations, it may be necessary to have departmental plans which integrate into one high-level plan. Further advice on plan presentation can be found in Chapter 5.

6.70. The method by which an incident management, business continuity or business recovery plan is invoked should be clearly documented. As part of this, the individual(s) that have the authority to invoke them should be recorded along with: how to mobilise the team(s); rendezvous points; and command centre locations.

6.71. Each incident management plan, business continuity plan and business recovery plan should set out prioritised objectives in terms of: the critical activities to be recovered; the timescales in which they are to be recovered; and the recovery levels for each critical activity.

6.72.   The purpose of a business continuity plan is to enable an organisation to recover or maintain its activities in the event of disruption. Invocation supports the critical activities of an organisation; plans may be invoked in whole or part and at any stage.

6.73.   **An Incident Management Plan** is a clearly defined and documented plan-of-action for use at the time of an incident. It should typically cover: task and action lists; emergency contacts; people activities; media response; stakeholder management; and locations. Other useful information to consider: contacts; mobilisation details for relevant agencies; log templates; maps, charts, plans and photographs.

6.74.   **A Business Continuity Plan** will typically contain: action plans and task lists, for example: how the BCP is invoked, who is responsible, the procedure, who does what when and where, services available, communications; resource requirements, for example: people, premises, technology, information and supplies; responsible person(s) and; forms, templates and annexes.

6.75.   **A Business Recovery Plan** aims to support the recovery and resumption of operations to a "normal" state. However, with some incidents it may not be possible to define what "normal" looks like until some time after an incident. Category 1 responders might, therefore, wish to ensure that BCPs are capable of extended operation, giving time for the development of recovery plans.

6.76.   The below diagram provides an illustration of how these three sorts of plan will come into play during a disruption.

Figure 6.2: Incident Timeline

BS 25999:2006 BRITISH STANDARD Business Continuity Management Part 1: Code of Practice [19]

Stage 5: Exercising, maintaining and reviewing BCM arrangements

6.77.   The Regulations require Category 1 responders to put in place arrangements to exercise BCPs to ensure they are effective.[20] An organisation's business continuity and incident management arrangements cannot be considered reliable until exercised.   Exercising is essential to developing teamwork, competence, confidence and knowledge, which is vital at the time of an incident. Arrangements should be verified through exercising, and a process of audit and self-assessment, to ensure that they are fit for purpose.

6.78.   When developing a BCM exercise programme, Category 1 responders will need to consider the:

     o   **focus** of the programme;

     o   **types** of exercise to be used

---

[19] Permission to reproduce extracts from [Name of Standard] is granted by BSI. British Standards can be obtained in PDF or hard copy formats from the BSI online shop: www.bsigroup.com/Shop or by contacting BSI Customer Services for hardcopies only: Tel: +44 (0)20 8996 9001, Email: cservices@bsigroup.com.
[20] regulation 25(a)

> o **involvement of senior management** in developing, executing and quality-assuring the programme;
>
> o **process** for delivering exercises; and
>
> o **relationship** between the BCM exercise programme and the exercising of emergency plans.

6.79.   Exercises should focus on impacts and test capabilities. While there is an infinite number of scenarios and possible responses, the list of impacts and capabilities is limited.

Figure 6.3: Types and Methods of Exercising BCM Strategies [21]

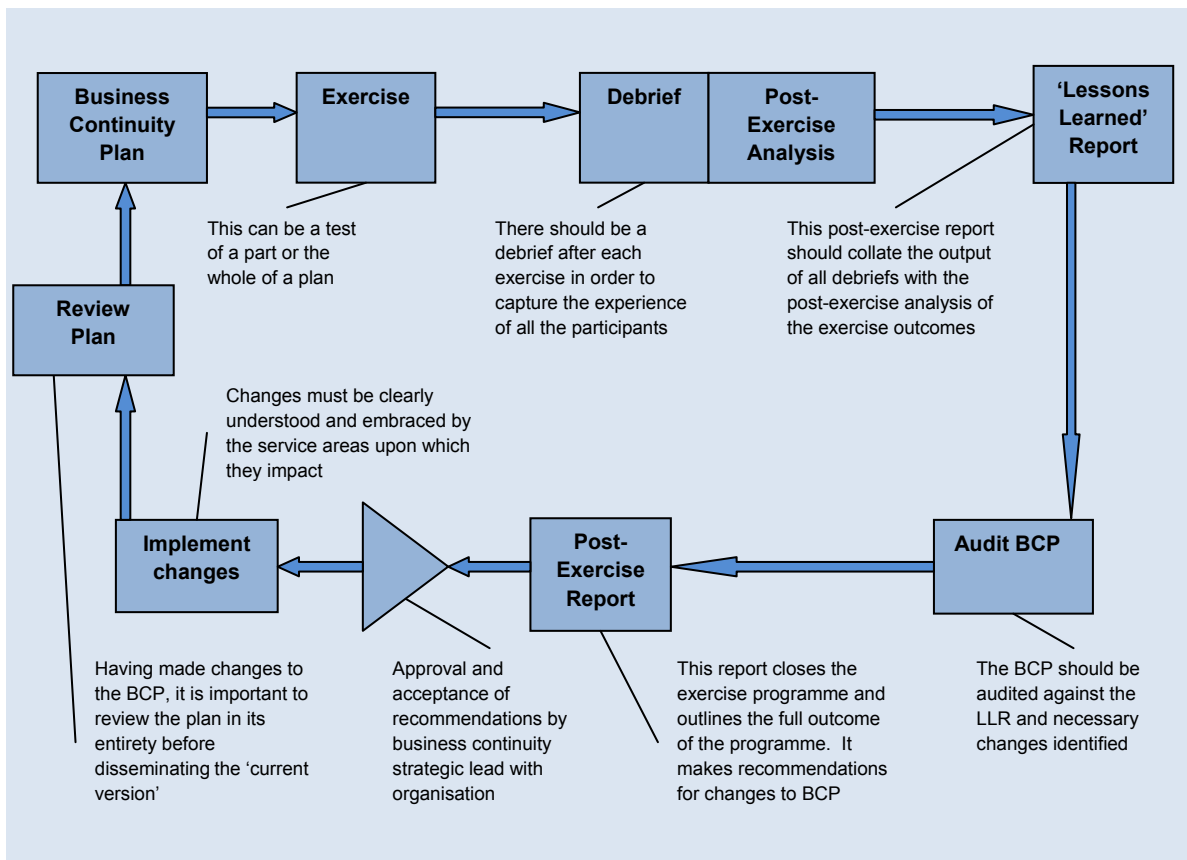| Complexity	Exercise	Process	Variants	Good Practice Frequency [1]
Simple	Desk check	Review/ amendment of content Challenge content of BCP	Update/validation Audit/verification	At least annually Annually
Medium	Walk-through of plan Simulation Exercise critical activities	Challenge content of BCP Use 'artificial' situation to validate that the BCP(s) contain both necessary and sufficient information to enable a successful recovery Invocation in a controlled situation that does not jeopardise business as usual operation	Include interaction and validate participants' roles Incorporate associated plans Defined operations from alternative site for a fixed time	Annually Annually or twice yearly Annually or less

[21] Regulation 4(4)(b), 4(7)

Last updated:March 2012

Complexity	Exercise	Process	Variants	Good Practice Frequency
Complex	Exercise full BCP including incident management	Building-/ campus-/ exclusion zone-wide exercise		Annually or less
The frequency of exercises should depend upon both the organisation's needs, the environment in which it operates, and stakeholder requirements. However, the exercising programme should be flexible, taking into account the rate of change within the organisation and the outcome of previous exercises. The above exercise methods can be employed for individual plan components, and single and multiple plans.				

6.80.   Exercising can take various forms, from a test of the communications plan, a desk-top walk-through, to a live exercise (See Figure 6.3 above). In all cases though, exercises should be realistic, carefully planned, and agreed with stakeholders, so that there is a minimum risk of disruption to business processes.

6.81.   The exercise programme should have the full support of the executive lead for business continuity issues. But the involvement of senior management should not be limited to defining the structure of the programme. In addition to taking part in exercises, senior management should be involved in quality-assuring the exercise programme and endorsing the outcomes.

6.82.   Figure 6.4 suggests a process for carrying out an exercise programme. Exercising is not about 'passing' or 'failing', it is all about learning lessons. There should be a debrief after each exercise in order to capture the experience of all the participants. What is important is that the captured data is recorded and considered as part of the post-exercise analysis.

Figure 6.4: Exercising your BCP – the learning cycle

6.83.   Every exercise should have clearly defined aims and objectives. A post-exercise debriefing and analysis should be undertaken which considers the achievement against these.

6.84.   The post-exercise analysis is usually undertaken individually by the exercise manager or as a meeting of the exercise-planning group. A post-exercise report should be produced that contains recommendations and a timetable for implementation.

6.85.   This report must be submitted to the executive lead for business continuity within the Category 1 responder organisation for approval of the recommendations.

6.86.   Once approval has been obtained, the changes to the BCP can be implemented. This should drive changes to the BCM and will be tested as part of any future exercising programme by the business continuity managers. This process provides the audit trail of BCP maintenance and testing.

6.87.   When exercising a specific part of a plan it may be more appropriate for the output to be a simple memorandum detailing the part tested. For example, for a call-out cascade exercise that tests the contacts listed within the plan for activation, a memo to the organisation's executive lead for business continuity that the test took place, was completed satisfactorily, and that all the contacts listed in the BCP are correct, would be sufficient to create the audit trail of that aspect of plan testing.

6.88.   It is important that business continuity planning and exercising are not done in isolation from wider emergency planning work. In part, BCPs are in place to ensure that Category 1 responders are able to deliver their emergency response function in the event of an emergency. Category 1 responders should not forget the close synergies between emergency plans and BCPs when learning the lessons of exercises and making changes as a result. Post exercise reports may have implications for both.

6.89.   The purpose of this exercise programme is to test the robustness of BCPs in the event of an emergency - will it enable the Category 1 responder to cope effectively with disruptions to the provision of critical services? One such critical function must be the emergency response function itself.

6.90.   The Act specifically requires Category 1 responders to maintain BCM plans to ensure that they can continue to deliver key services in the event of an emergency. It is essential that Category 1 responders must not only put plans in place, but also ensure that they are regularly reviewed and kept up-to-date.

6.91.   Plan maintenance should therefore be an ongoing process. It is good practice to undertake a comprehensive review of the state of the plan periodically.

6.92.   A process should be established whereby the BCM team is informed of relevant changes and developments, and that these are incorporated into the plan. Effective version control procedures should be implemented to ensure that relevant members of staff are working from the correct edition of the plan.

Stage 6: Embedding BCM in the organisation's culture

6.93.   Documenting the BCP is one element of developing a BCM strategy. Its success, however, depends upon:

- o **implementation** of the recommendations made, across the entire organisation;
- o a programme of **training** for those directly involved in the execution of the plan; and
- o an **education and awareness programme** to ensure understanding and adoption of the plan in relevant parts of the organisation - this applies to both internal and external stakeholders (e.g. employees and suppliers).

6.94.   Category 1 responders should deliver a programme of training and awareness to ensure that the relevant parts of the organisation are confident and competent concerning the plan. All parties must appreciate the importance of BCM to the operation's survival and their role in this process. This means that business continuity should be 'mainstreamed' in emergency management and should be a core element of the emergency planning culture the Act establishes.

6.95.   As the first part of this chapter notes, the Regulations require Category 1 responders to give appropriate training to those involved in implementing BCPs.[23] This section of the chapter also sets out the objectives of such training programmes and what they should cover.

6.96.   Training will need to be done on a rolling basis to cover staff turnover. BCM co-ordinators should establish a training database to monitor the take-up of training opportunities.

6.97.   It is also important to ensure that awareness of BCM issues is raised throughout the organisation, to ensure that all relevant staff have confidence in its ability to manage in a crisis, and know how they should respond in the event of a disruption. For example, some organisations distribute 'z-cards' to all staff, setting out what they should do in the event of a range of contingencies (e.g. details of secondary sites or evacuation points). The box overleaf sets out some of the key messages and the means of getting them across.

---

[23] regulation 25(b)

Box 6.1: The Business Case for BCM

Part of embedding a 'continuity culture' within an organisation is to convince senior staff of the business case for BCM. It makes sense to put in place BCM arrangements because they help to:

- o **protect the reputation of the Category 1 responder.** The community expects continuity of critical services, even in the most challenging of circumstances. They expect you to be fully in control, and to be seen to be in control - your organisation's reputation is at risk if you are not. Maintaining the reputation of statutory services in an emergency is a vital element for public reassurance;

- o **produce clear cost benefits.** Identifying, preventing and managing disruptions in advance can reduce the costs to an organisation in terms of financial expenditure and management time. The demands of the insurance market have also increasingly become an important driver;

- o **protect the organisation, ensuring that Category 1 responders can help others in an emergency.** For Category 1 responders to help others, they first have to be able to keep themselves going in the face of a disruption. BCM will help ensure that they can mobilise the capabilities they need to deal with the emergency. It will also help ensure that the impact of the emergency on the day-to-day functions of the Category 1 responder is kept to a minimum, and that disruptions to vital services do not deepen the impact of the emergency on the wider community;

o **ensure compliance and corporate governance.** Category 1 responders are - to varying degrees - subject to performance standards, corporate governance requirements and, in some cases, specific requirements to do BCM (e.g. NHS Trusts). Establishing BCM arrangements pursuant to the requirements of the Act will help ensure compliance with this wider framework of responsibilities and expectations; and

o **develop a clearer understanding of how the organisation works.** To ensure the continuity of an organisation, you first have to understand how it works. The process of analysing the business can yield sources of increased operational effectiveness and efficiency.

6.98.   To be truly effective, BC must form part of the culture in an organisation. This can be achieved by: leadership from senior personnel; assigning clear responsibilities; awareness raising; skills training; and exercising plans.

6.99.   Category 1 responders should extend their awareness-raising activities to those third parties upon whom the Category 1 responder depends in both normal and crisis operations. They need to be aware of how the response will develop when a BCM event occurs, and what this will mean for them.

6.100.   Category 1 responders also have an interest in ensuring that their suppliers and contractors have in place robust BCM arrangements. To ensure the resilience of operations, it is necessary to ensure that other aspects of the delivery chain are resilient too. It is important to build BCM into procurement and contract management processes. The Office of Government Commerce provides detailed advice on these issues which is freely available on its website: http://www.ogc.gov.uk.

6.101.   Business continuity as part of Civil Protection is very much a multi-agency activity, where Category 1 responders must work together - and understand each other's capabilities and vulnerabilities - if they are going to be effective.

6.102.   In the emergency planning area, it is essential for Category 1 responders to be aware of each other's plans. BCM arrangements underpin emergency management capabilities - it is important that Category 1 responders have an awareness of the continuity issues facing their partners in the event of an emergency. Which functions will be discontinued? How will functions be scaled down or up in the event of an emergency? Where are partners' contingency sites?

6.103.   The Local Resilience Forum (LRF) provides a framework for dialogue about business continuity issues. Category 1 responders should consider using the LRF process as a means of raising mutual awareness, ensuring that plans dovetail, developing frameworks for mutual assistance, and sharing best practice.

6.104.   The Act requires Category 1 responders to publish aspects of their BCPs in so far as this is necessary or desirable for the purposes of dealing with emergencies.[24]

6.105.   The purpose of this requirement is to ensure that Category 1 responders make relevant information available to the public about what will happen in the event of an emergency. There are three principal classes of information which Category 1 responders should consider communicating to the public:

> o   a descriptive account of the business continuity plans they have in place for the purposes of reassuring the public;

[24] s.2(1)(f)

Last updated:March 2012

- o information about the implications of emergencies for the continuity of a Category 1 responder's ordinary operations – e.g. possibility of service suspensions or adjustments. Proactively publishing this sort of information in advance of an emergency allows the public to think about their preparations. For example, parents might find it useful to know under which circumstances schools might be closed in the event of severe weather;

- o sources of information and advice about service continuity issues that the public could consult in the event of an emergency.

6.106.   This communication can take place through a variety of means, including websites and other publications. This could also be achieved by integrating business continuity issues within mission statements, statements of service and other public information brochures, relating either to the organisation as a whole or to individual services.

6.107.   Responders can get further guidance and support from the following website http://shop.bsigroup.com/. In particular, the British Standard on business continuity, BS25999 parts 1 and 2, will be useful along with PB25666: Guidance on exercising and testing for continuity and contingency programmes.

6.108.   The International Standards Organisation (ISO) are in the process of producing a requirements and guidance document on business continuity; ISO22301 and ISO22313. Publication of these two documents has not been agreed. Early indication is however that if published, there will be nothing substantially different to the British Standard BS 25999, parts 1 and 2. Therefore, alignment with the British Standard will not only provide a good basis for BCM but at this stage would also appear to align with the forthcoming international standards.