Business Continuity

A Framework for
NHS Scotland

Strategic Guidance for NHS Organisations in Scotland

Contents

1 Introduction

The Civil Contingencies Act (CCA) 2004 established a new legislative framework for civil protection within the UK. The Civil Contingencies Act (Contingency Planning) (Scotland) Regulations 2005 describes how the provisions of the act apply in Scotland. Both place a clear obligation on Category 1 organisations within NHS Scotland to respond to disruptive challenges. However, with increased risks, there is a need to ensure that all Category 1 and Category 2 organisations within NHS Scotland together with those providers who supply a critical service to NHS Scotland (e.g. GP Practices, Dental Practices, Pharmacies, Care Homes etc.) are sufficiently resilient to respond to any threat. Consequently there needs to be a robust system in place within all organisations to plan, exercise, and review their response against a range of disruptive challenges. Business Continuity Management (BCM) is an essential component of this resilience and a requirement of the CCA.

In the last ten years, a number of incidents such as bombings, extensive flooding and consequent loss of power, water and telephony, and flu outbreaks, have drawn attention to the importance of resilience planning. The Pitt Review – Learning Lessons from the 2007 Floods in the UK emphasised the need for a systematic approach to the risk of flooding, the need to maintain critical services and business in the light of such emergencies and to have in place the means for communities to be able to recover from such events. The Report also emphasised to all organisations the need to ensure effective Business Continuity Plans (BCP's) are in place. The implementation of effective BCP's in a crisis situation is seen as an invaluable step in making sure critical services are maintained for as long as possible, or if lost, can be recovered as quickly as possible.

This Guidance is built on current good practice and shared knowledge and is intended to:

- Improve BCM resilience within NHS Scotland.
- Ensure through the adoption of resilience principles the continuous operational delivery of critical healthcare services when faced with a range of disruptive challenges e.g. staff shortages, denial of access, failures in technology, loss of utility services and failure of key suppliers.
- Help drive NHS Scotland's compliance with the CCA.
- Allow a unified and cohesive approach to BCM which parallels the British Standard BS 25999 and develop a resilient healthcare system.

The Guidance describes a set of general principles and provides a common baseline for NHS Boards and other NHS Scotland organisations to follow when developing their ability to achieve BCM within the context of the requirements of the CCA to:

- Continue to perform their functions and provide patient care and services in the event of an emergency so far as reasonably practicable.
- Be able to maintain their own emergency response capabilities and to continue to deliver critical services.

Chief Executives of NHS Boards have responsibility for BCM, which includes ensuring that arrangements made within their boundaries are adequate and appropriate to local circumstances. This Guidance gives the Chief Executive of each NHS Board the responsibility for ensuring that their organisation has a BCM process in place that will address the requirements for ensuring business continuity as required by the CCA. Similarly, it is recommended that any organisation that provides services to NHS Scotland for patient care also have adequate arrangements appropriate to the size and type of the organisation.

This document focuses on planning, preparing and responding in the NHS in Scotland. However, it is recognised there is a need for a high level of networking with service providers in other parts of the United Kingdom in order to support mutual aid arrangements.

1.1   Business Continuity Overview

BCM is a process which provides a framework to enhance the resilience of organisations and businesses to any eventuality, to help ensure continuity of service to patients and customers and the protection of the NHS Scotland brand and reputation. It provides a basis for planning to ensure long-term survivability following a disruptive event. These events can be either internal or external and can, if not correctly managed, lead to major disruptions to critical services BCM should be part of the way NHS Scotland organisations perform their day to day business. It is better to plan for challenges which may affect the organisation rather than have to "catch-up" when an event occurs.

BS 25999 defines BCM as

> "the capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at acceptable pre-defined levels within agreed time frames".

For NHS Scotland, interruption may be defined as:

> *"Any disruptive challenge that threatens personnel, buildings or the operational procedures of an organisation and which requires special measures to be taken to restore normal operating functions".*

BCM is concerned with ensuring organisations can continue operating to a pre-determined level in the event of a major disruption. Effective BCM is, therefore, not only about minimising the likelihood of an event occurring but also having the ability to recover and restart if the worst happens. The consequences of not having effective BCP's in place could have serious implications, including:

- Failure to deliver critical services.
- Loss of life or injury.
- Lengthy restoration times.
- Loss of public confidence.
- Exposure to potential legal action.

BCM should be considered as a continuous process, which needs to be embedded within the organisation's culture (Business Continuity Management Life Cycle, BS 25999).

Business Continuity
Management Life Cycle
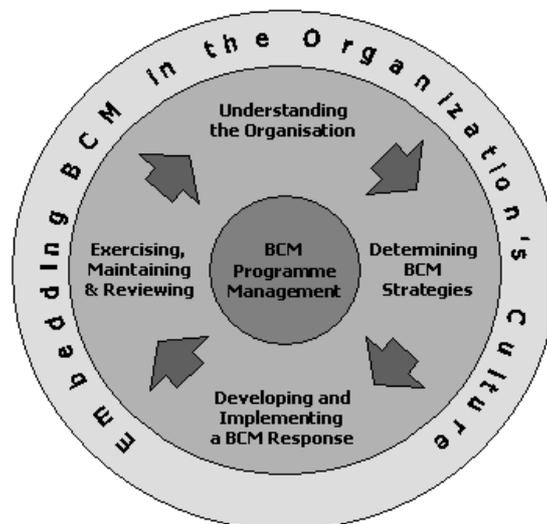
2   Roles and Responsibilities

BCM forms an important part of risk management and is a requirement of the
CCA.

BCM, including processes for recovery and restoration, should be considered by
an organisation as part of its every day business processes. BCM should be
embedded in the culture of the organisation as are the principles of health and
safety, and there must be demonstrable commitment to the process. The skills to
develop BCM processes can be seen as complementary to those involved in
emergency management but the duty may in some cases be undertaken by
separate officers. It is critical though that both processes, where appropriate, are
integrated and complementary to each other as a major incident may occur at the
same time as a business continuity issue, or be triggered by it.

The key principles for maintaining BCM are:

- Review critical services and identify resources which need to be available
  to maintain critical services for the first hour, 24 hours, 3 days and for 7
  days.
- Assess progress on BCM processes against an agreed checklist.
- Establish contracting processes with providers and suppliers that require
  BCM processes to be explicitly described and covered by contracts.

2.1   Scottish Government (SG)

The SG has a responsibility to promote the implementation of BCM across NHS
Scotland. In addition, SG has a responsibility to review the BCM arrangements
of NHS Boards in Scotland designated as Category 1 Responders in terms of
the Civil Contingencies Act 2004. The SG also has a responsibility to maintain
the currency of BCM guidance to ensure that the guidance reflects best practice.

2.2   NHS Boards

NHS Boards are accountable to the Scottish Government and the public for the
effective functioning of the NHS within their respective areas. They provide the
local management function for NHS Scotland and operate as both providers and
contractors of services for their area.

NHS Boards must ensure the highest level of patient care is maintained
regardless of circumstances on a 24 hour a day, 7 day a week basis.

Section 2 (1)(c) of the CCA imposes a statutory duty on NHS Boards (Category 1
Responders) to maintain plans for the purpose of ensuring, so far as reasonably
practicable, that if an emergency occurs, it is able to continue to provide critical

services. NHS Boards must also ensure that all contracted service providers are capable of providing critical services at an appropriate level.

For those NHS Scotland organisations not designated as a Category 1 Responder, and which are not obliged under the CCA to have BCM arrangements in place (e.g. certain Special Health Boards), it is considered good practice for them to have these arrangements in place as an essential part of their Clinical Governance and Risk Management arrangements.

2.3   Service Providers

Service providers contracted by NHS Boards should be able to demonstrate adequate arrangements are in place and where appropriate provide evidence to ensure continuity of an acceptable level of service. Compliance or certification to BS25999 by service suppliers may provide some assurance of their BCM capability.

3   Guidance on BCM

BCM adopts the principal of building on what already exists within an organisation. Organisations within NHS Scotland have historically utilised informal "workarounds" which enable critical services to be delivered at a time of disruption. BCM ensures these are integrated into a formal process to enable a faster and more effective response to be deployed to maintain and/or recover critical services.

BCM is a business-owned, business-driven process which establishes a fit for purpose strategic and operational framework that:

- Proactively improves an organisation's resilience against disruption of its ability to achieve its key objectives.
- Provides a rehearsed method of restoring an organisation's ability to supply its critical services to an agreed level within an agreed time after a disruption.
- Delivers a proven capability to manage business disruption and protect the organisation's reputation and brand.

Having a planned response to disruptive challenges will enable NHS organisations ensure critical services are maintained, and the organisation's reputation is protected.

BCM arrangements can benefit an organisation because they help to:

- Develop a clearer understanding of how the organisation works. This process of analysing the business can yield sources of increased operational effectiveness and efficiency.
- Protect the community by ensuring the impact of disruptive challenges on service delivery is kept to a minimum.
- Maintain Clinical Governance thus providing assurance that the organisation has systems and processes to maintain patient services and delivery.
- Protect the reputation of the organisation.
- Produce clear cost benefits. Identifying, managing and preventing disruptions in advance can reduce the costs to an organisation in terms of financial expenditure and management time.
- Ensure CCA compliance and demonstrate good corporate governance.
- Enable performance standards and key performance indicators to be maintained.

A successful BCM process will:

- Identify and protect critical activities and supporting services ensuring their continuity.

- Provide an incident management capability that reduces the risk of incidents becoming crises.
- Provide the organisation with an understanding of itself, its relationships with its partners, suppliers, other organisations, including the emergency services, is properly developed, documented and understood.
- Ensure staff are trained to respond effectively to an incident or service disruption.
- Ensure stakeholder requirements are understood and satisfied through effective delivery of their requirements.

Effective BCM is built on the "Seven P's". (Emergency Preparedness, Cabinet Office Civil Contingencies Secretariat, 2005):

1. Programme – proactive management of the BCM process.
2. People – clear understanding of roles and responsibilities through awareness and education.
3. Processes – understanding of how the organisation operates.
4. Premises – buildings, facilities and equipment.
5. Providers – clear understanding of the organisation's supply chain, including outsourcing and utilities.
6. Profile – protection of the organisation's image and reputation.
7. Performance – evaluate performance by benchmarking and audit.

3.1   BCM in a Multi-Agency Environment

When organisations within NHS Scotland are developing BCM, it is essential they consider the external environments in which the organisation operates. In particular, organisations are required to work with other responders. BCM strategies and plans must recognise and accommodate the influence of these external environments.

The following model can help identify the areas which may have influence on the organisation:
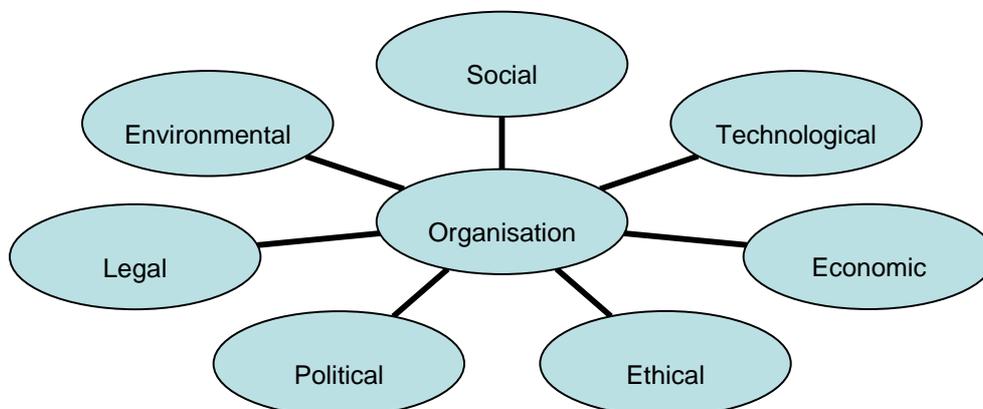
NHS Scotland organisations should:

1. Where applicable, work as part of a multi-agency response via their local Strategic Co-ordinating Group (SCG).

2. Risk assessment is identified within the CCA as an essential step in the emergency planning and business continuity process. It ensures that local responders develop plans which are sound and proportionate to identified risks. Within each Strategic Co-ordinating Group, NHS Scotland organisations have responsibility in the context of multi-agency planning to contribute to the Community Risk Register (CRR). Organisations within NHS Scotland therefore need to undertake risk assessments appropriate to their facilities and critical services.

3. Undertake its own internal risk assessment in order to inform its own response and to provide an input to the multi-agency risk assessment (see section 4.2.3).

An agreed methodology for risk assessment is available on the Cabinet Office website.

http://www.ukresilience.gov.uk/preparedness/risk.aspx

3.2   Linking BCM and Sustainable Development

In addition to making NHS Scotland more resilient to disruptive challenges, there is also a need to ensure NHS Scotland considers its impact on the environment through reducing, where possible its carbon footprint. Whilst it will not always be possible to produce resilience without totally eliminating the environmental impact, through innovatively linking the resilience and sustainable development agendas, certain solutions can compliment both policy areas. For example, the use of micro power generation on site will not only provide a reduction in environmental impact, but also provide an alternative (albeit small) residual power supply source. It is recommended that BCM leads within NHS Scotland organisations work closely with those colleagues involved with sustainable development to try to maximise the links between these two policy areas.

4   The Key Stages of BCM

There are 5 key stages to be followed to establish BCM processes successfully into NHS Scotland organisations:

Stage 1 – Programme Management

This enables the business continuity capability to be both embedded and maintained in a manner appropriate to the size and complexity of the organisation and to comply with the Quality Improvement Scotland (QIS) National Standards for Clinical Governance and Risk Management.

Responsibility – Chief Executive and other Board Members	⟶	Initiate and maintain the BCM process
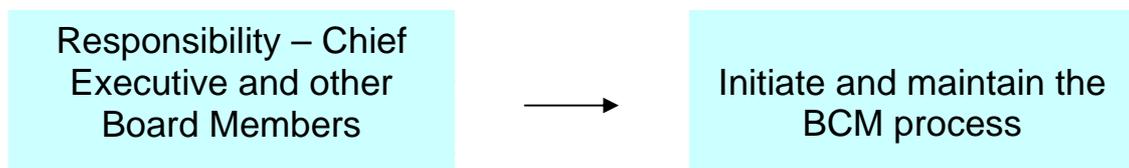
Stage 2 – Understanding Your Business

The use of business impact and risk assessments to identify critical services, evaluate recovery priorities and assess the risks that could lead to a disruption of critical services.

Responsibility: Strategic Directors, Senior Managers and Operational/Service Leaders

Business Impact Analysis	Risk Assessment
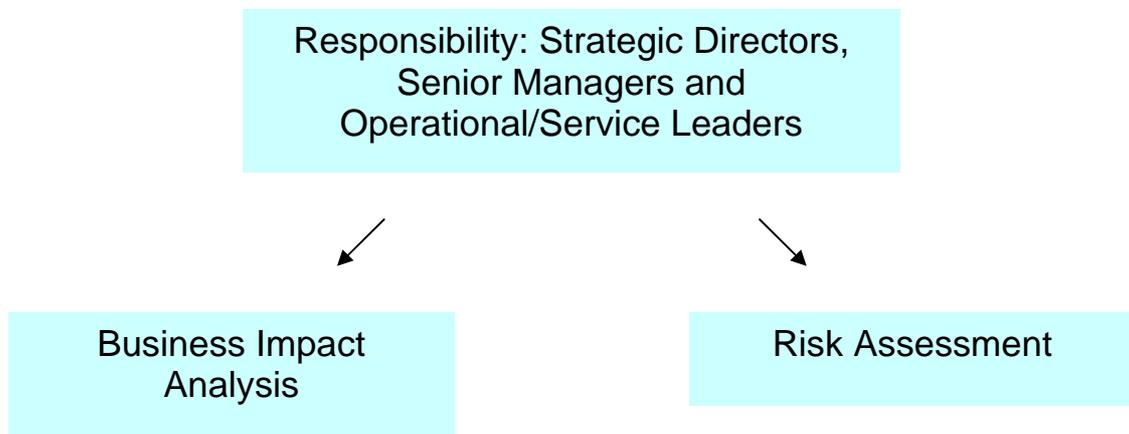
Stage 3 – Determining BCM Strategies

Identify alternative strategies available to mitigate loss and assess their potential effectiveness in maintaining the ability to deliver critical services.

Responsibility: Strategic Directors/Senior Managers/Operational and Service Leads/ BCM Planners	→	Selecting options for analysis
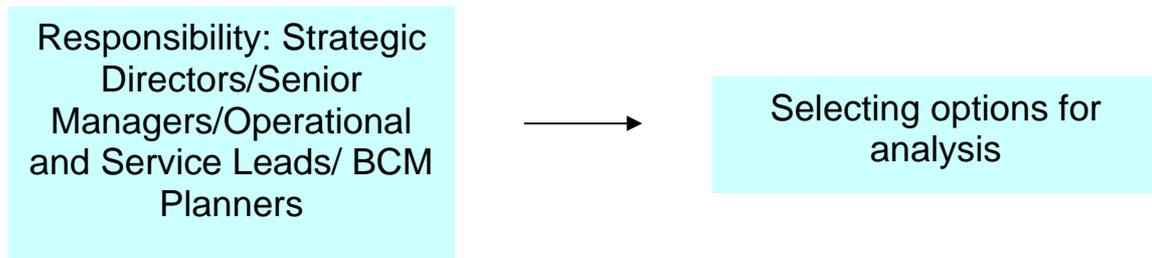
Stage 4 – Developing and Implementing a BCM Response

The development of plans in response to business continuity challenges and the plans underpinning this.

Responsibility: Strategic Directors/Senior Managers/Operational and Service Leads/ BCM Planners → Implementation Planning

Implementation Planning
- Develop Business Continuity Plans
  - Develop Procedures
    - Education, Awareness and Training
- Implement Risk Reduction Measures
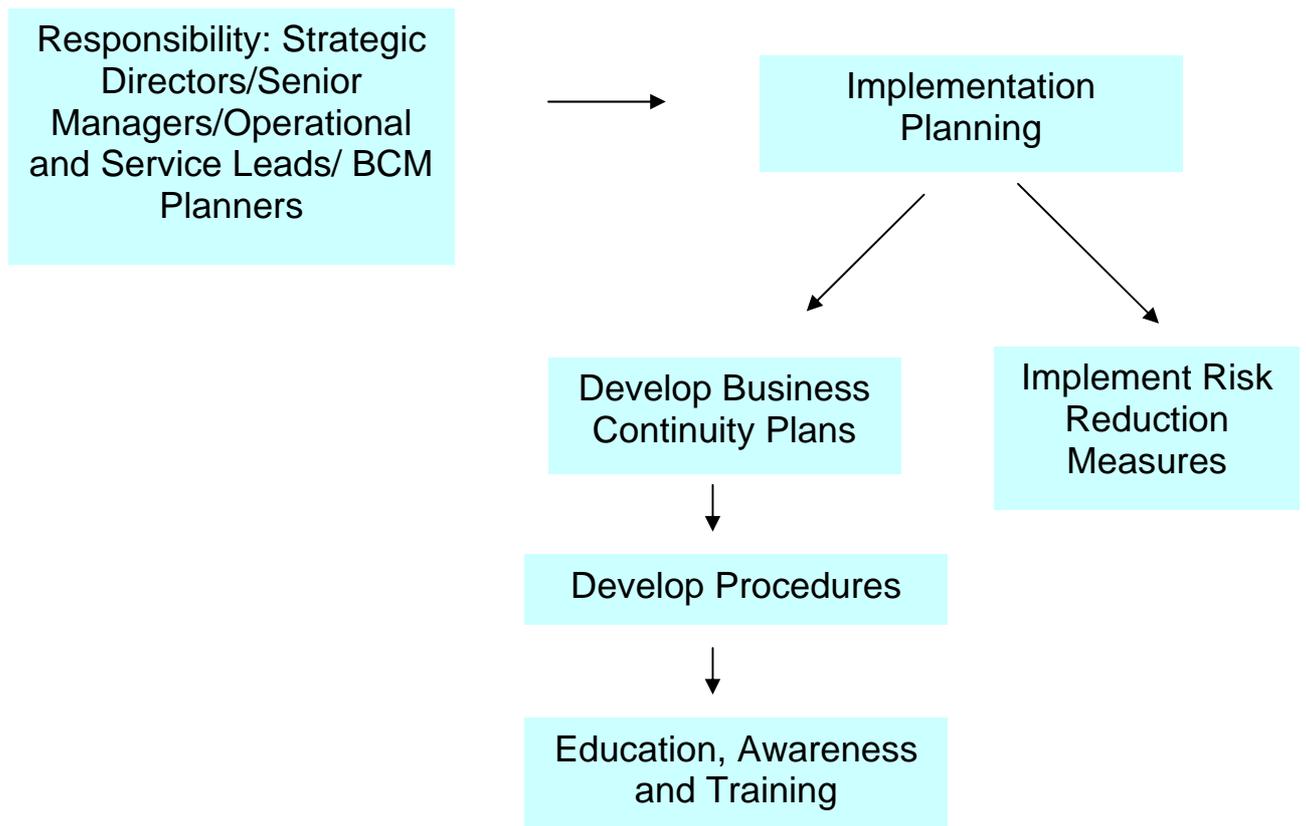
Stage 5 – Exercising, Maintaining, and Reviewing

Ensure plans are fit for purpose, updated, and quality assured.

Responsibility: All Staff	→	Exercise Resilience Planning Arrangements	→	Keep Plans Up To Date

↓

Self-Assessment and Audit of Plans
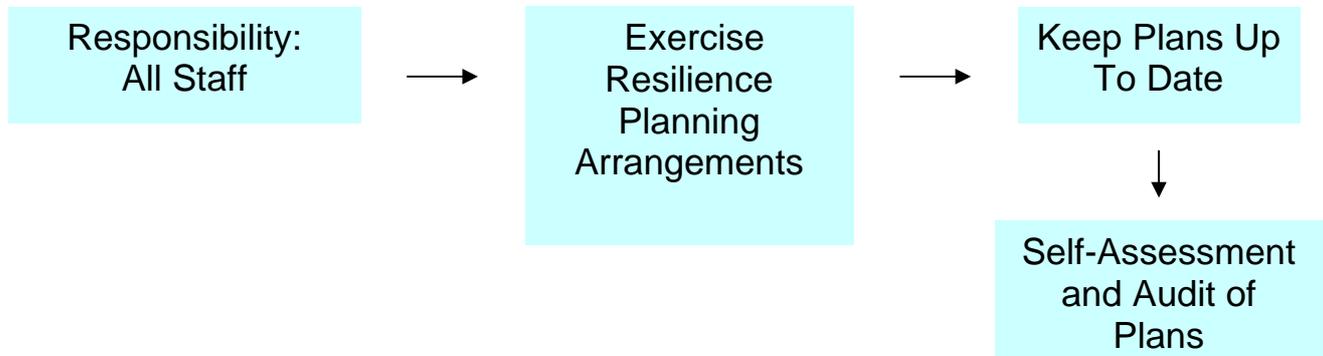
4.1   Stage 1 – Programme Management

BCM must be regarded as an integral part of the normal management process. The organisation's Senior Management must regard BCM arrangements as essential and their support provides crucial decisions:

- On the scope of BCM within the organisation
- Policy direction and resource provision to enable BCM to be established, maintained and embedded within the organisation.
- Ensuring commitment throughout the organisation in order for BCM arrangements to be effective.
- About attitudes to risk and service prioritisation that can only be taken at the top level.
- Ensuring effective governance arrangements are in place.

4.1.1 Responsibilities

Each NHS Scotland organisation must:

- Appoint or nominate a person with appropriate seniority and authority (e.g. Board Level Director) to be accountable for BCM policy and its implementation.
- Appoint or nominate one or more individuals to implement and maintain the BCM programme. These individuals should represent all areas of the organisation.

Each individual has responsibility for BCM within the organisation. These responsibilities are:

- The Chief Executive (or equivalent) has overall accountability for the successful implementation and maintenance of BCM for the organisation.
- The BCM Lead Director has overall responsibility for the successful implementation and maintenance of BCM for the organisation.
- Board Directors have responsibility for the successful implementation maintenance of BCM for the critical services within their areas of responsibility.
- Heads of Divisions/Teams/Business units/other have responsibility for oversight of the BCM implementation and maintenance within their area of responsibility.
- Local Managers are responsible for successful implementation and maintenance of BCM within their area of responsibility.
- Each individual employee is responsible for ensuring that he/she is familiar with the BCM plan and his/her role within it.

This ensures the profile of BCM issues is appropriate and decisions are made at a suitable level. BCM is an ongoing process and it is important to gain the support and endorsement of the organisation at the end of each stage. It is the responsibility of senior management to provide the assurance that BCM arrangements are robust.

4.1.2 Programme Maintenance

The BCM Programme must be designed to ensure that business continuity is embedded within the organisation and BCM becomes part of every service managers' normal responsibilities. The programme must also ensure each component of an organisation's business continuity capability is regularly reviewed, exercised and updated (see section 4.5).

BCM arrangements and plans must be reviewed and updated whenever there is a significant change in the organisation's operating environment, personnel, processes or technology, and when an exercise or incident highlights deficiencies. Lessons identified from exercises or incidents carried out by other organisations should also be incorporated,

4.1.3 Organisational Culture

The outer part of the BCM life cycle (see section 1.1) relates to an organisation's culture. BCM must become part of the way an organisation is managed, regardless of size or function within NHS Scotland. At each stage of the BCM process, opportunities exist to introduce and enhance an organisation's BCM culture.

An organisation with a positive BCM culture will gain benefits, as it will:

- Develop a BCM programme more efficiently.
- Instil confidence in its stakeholders, especially staff, patients and customers, in its ability to handle disruptive challenges.
- Increase its resilience over time by ensuring BCM implications are considered in decisions at all levels for existing and new services.
- Minimize the likelihood and impact of disruptions.

To be successful, BCM must be "owned" by everyone within the organisation. Many disruptions to critical services within NHS Scotland organisations are caused by internal failures. Organisations must adopt a culture to encourage staff at all levels to participate in the identification of alternate methods of working if normality is disrupted. Where appropriate, these ideas should be incorporated into business continuity plans.

All staff must be convinced that BCM is a serious issue for the organisation and they have an important role to play in maintaining the delivery of critical services to their patients. It is essential awareness programmes are established as part of the overall establishment of BCM.

4.1.4 Awareness

To be successful, the BCM Programme must include processes that:

- Ensure all personnel are aware of how they contribute to the achievement of the organisation's business continuity objectives.
- Raise, enhance, and maintain awareness by establishing an ongoing BCM education and information programme for all staff including new recruits.
- Introduce a process for recording and evaluating the effectiveness of BCM awareness delivery.

Organisations may consider placing BCM within individual's personal objectives.

4.1.5 Training

BCM training is a statutory requirement placed on NHS Scotland under the CCA.

The BCM Programme must incorporate processes for identifying and delivering the BCM training requirements of relevant participants. In addition, the BCM Programme must also record and evaluate the effectiveness of the training delivery.

Good practice guidance on BCM training can be found at:

http://www.ukresilience.info/preparedness/ccact/good_practice/awareness_training.aspx

4.1.6 Documentation

A key element of Programme Management is the control and management of documentation. Within BCM, this is critical since, at the time of any disruption, it is essential that all players have access to, and work from, authorised and current incident or continuity plans and supporting documentation.

Some of the information contained within the BCM documentation will be of a sensitive nature and therefore must be subject to appropriate protection and confidentiality markings.

The management of the organisation must therefore establish and maintain a documented and controlled system of document and records management covering identification, storage, protection, retrieval, retention time and disposal of documents and records in accordance with the latest guidance.

4.2   Stage 2 – Understanding Your Organisation

An accurate assessment of the organisation and its critical services is essential, as it provides the basis upon which all subsequent BCM strategies and plans are based. Key questions should include:

- Who are the key stakeholders and what are their expectations?
- What are the critical services that enable the NHS Scotland organisation to meet it's most important and time-sensitive objectives?
- What are the essential activities i.e. those supporting activities which must be performed to deliver the critical services?
- What processes are used to deliver essential activities?
- Who and what is used in these? (Such resources can be either internal or external to the organisation.)
- What is the impact over time on the community and the organisation if critical services and essential activities for whatever reason are disrupted?

In addition, it is important to put in place a process for identifying critical services whose loss would have the greatest impact in the shortest time, which need to be recovered most rapidly, and for identifying acceptable levels of service provision. If a declared set of aims, objectives and targets exists for the organisation, this will help identify critical services the BCM process should focus upon.

Critical services should be considered from a patient and customer perspective. In addition, these critical services should be considered on an "end to end" basis.

The critical services may require many players, both internal and external, to ensure delivery to patients and customers and it should be recognised that an interruption to any element of the service may threaten the delivery of the overall service.

BCM requires an understanding of activities, processes, and resources required for the delivery of critical services. Critical services may have many dependencies both internally and externally. These can include customers, suppliers, partners, agencies, and other services provided internally by the organisation itself. It is important to identify these at an early stage and to take their impact into account. The involvement of representatives from these key dependencies on the BCM planning team will add significant value to the process.

4.2.1 Business Impact Analysis

Once the essential activities and resources that support the critical services have been identified, it is important to determine what the impact would be upon the organisation's goals and targets if these were disrupted or lost. This stage is known as Business Impact Analysis (BIA). BS 25999 defines BIA as "the process of analysing business functions and the effect that business disruption might have upon them".

BIA is a crucial element in the implementation and underpinning of the whole BCM process. BIA is a process that identifies, quantifies, and qualifies the impacts and their effects on a service due to loss, interruption or disruption of an essential activity and its' supporting processes and resources, and helps measure the impact of disruptions over time on the organisation. It provides information which underpins later decisions for business continuity strategies.

There are five key elements to the BIA process:

- Defining activities and their supporting processes and resources.
- Mapping distinct stages of each activity and process.
- Determining impacts of a disruption over time.
- Defining recovery time objectives [BS 25999 defines Recovery Time Objective (RTO) as the target time set for the resumption of a service delivery after an incident].
- The minimum resources required to meet those objectives.

The purpose of the BIA is to:

- Identify and understand the organisation's critical services, and the priority of each.
- Quantify the maximum tolerable period of disruption [The Maximum Tolerable Period of Disruption (MTPoD) is defined within BS 25999 as the

duration after which the organisation's viability will be irrevocably threatened if the service cannot be resumed] for each service, i.e. the timeframe during which a recovery must become effective before an outage compromises the ability of the organisation to achieve its business objectives. This evaluation must fully consider the organisation's contractual, regulatory, and statutory obligations. The Recovery Time Objective (RTO) must be less than the MTPoD.

- Provide resource information from which an appropriate recovery strategy can be determined.
- Outline the dependencies that exist, both internal and external, which are required to provide the critical services.
- Quantify the resources required, over time, to maintain the critical services at an acceptable level.

4.2.2 The BIA Process

The scope of a BIA process should:

- Identify if more than one team (both internal and external) is involved in the service provision and the relationship between these teams.
- Identify the key service objective(s) and success criteria of each team.
- Confirm the incident scenarios to be investigated e.g. loss of staff, loss of premises, technology failure, building service failure, supplier failure, loss of utility, and possible combinations of these.

The organisation's critical services should be analysed to:

- Identify the key processes across service areas and managers of these services.
- Identify the service subject experts from whom information can be sought about the key processes.
- Identify the impacts of a disruption of critical activities and key processes on the service.
- Quantify the timescale within which the interruption of each critical service becomes unacceptable.

The impact of potential disruptions should be priority rated by considering the following:

- Implications for critical service delivery.
- Health, welfare and safety of stakeholders.
- Reputation.
- Environmental implications.
- Statutory and legal obligations.
- Financial cost to the organisation.

- Impact of disruption on partner organisations.

The BIA should identify and document:

- The aims, objectives, and impact on the critical services of the organisation.
- Dependencies (including seasonal trends) and/or key timing issues for critical services.
- Financial and non financial impacts and effects/consequences resulting from disruption of the critical services over various time periods.
- The BCM objectives for each critical service and its dependencies.

The BIA must consider:

- Staff numbers and key skills.
- Vital records/data (all media).
- Technology, including IT.
- Consumables / pharmaceuticals.
- Facilities.
- Key clients and stakeholders.
- Suppliers.

The output from this element of the process is used to advise internal and external functions of the resource requirements of the critical service at a time of disruption. The BIA provides information to enable facilities, IT and other key functions to develop their continuity plans to meet the critical service needs.

4.2.3 Risk Assessment

By following the previous stages of the BCM process, the organisation will have identified its critical services and their esential activities, processes and supporting resources. The next stage in the process is risk assessment. Risk assessment is undertaken at this stage to ensure the BCM effort is focussed on those critical service elements most at risk and/or those service elements that would have the greatest impact if the risk materialises.

BCM risk assessments use established risk assessment techniques and should identify internal and external threats, single points of failure (which may be people related, facilities, information technology, utilities, suppliers, etc). The risk assessments should also take account of the Scottish Environment Protection Agency's local flood maps, the CCA, BCM Planning Assumptions, and the local Community Risk Register (CRR).

Information from the risk assessments and the BIA should be combined to:

- Produce a system which identifies those areas where the organisation's initial BCM effort should be concentrated.
- Identify measures that:

  a)   Reduce the likelihood of a disruption.
  b)   Shorten the period of disruption.
  c)   Limit the impact of a disruption on the organisation's critical services.

Risk assessment matrices are provided (Annex 4).

Such measures are known as loss mitigation and risk treatment. Loss mitigation and risk treatment strategies may be used in conjunction with other options, since not all risks can be prevented or reduced to an acceptable level.

Organisation's should decide on the approach to be taken to protect the operation of critical services. The nature of the risk, defined in terms of its likelihood and impact, will determine which action is appropriate and what, if any, action is required. Disruptions that are low likelihood and low impact may require no specific action and can be dealt with through generic arrangements. However, risks that are high impact and high probability may need specific plans and risk mitigation strategies.

Strategies which organisations may adopt are:

- Do nothing/accept.
- Mitigate by management/containment.
- Prevent/reduce by change/transfer or end the process.
- Plan for business continuity.
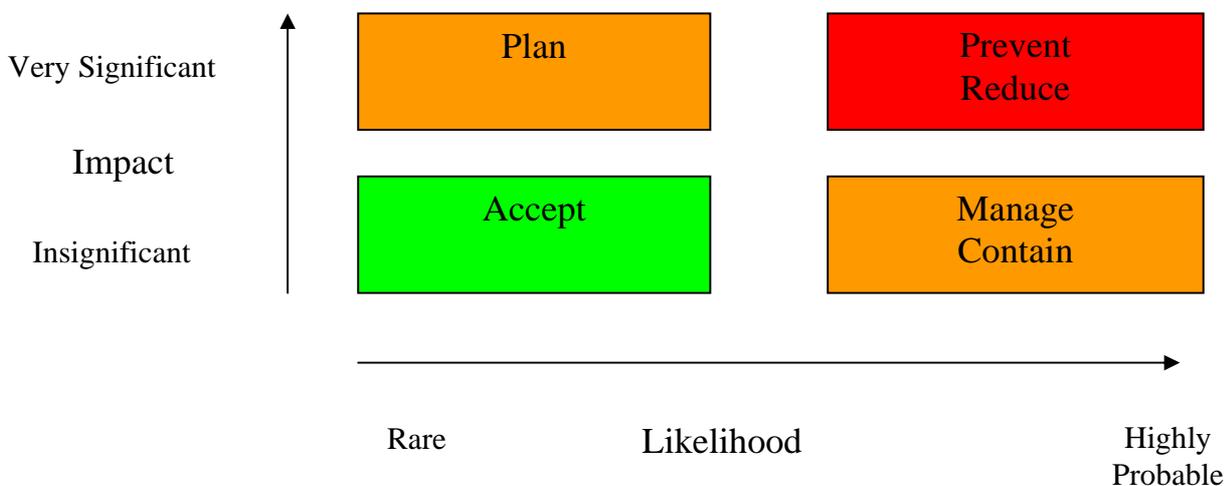
The organisation's senior management must agree and sign off the business impact analysis and risk assessments. Any significant risks that have been identified, as part of this process, must be incorporated into the organisation's risk register

4.3   Stage 3 – Determining BCM Strategies

BCM strategies determine how operational continuity is to be achieved. Such strategies are based on:

- The critical services and the essential activities, processes and resources that support these.
- The business impact analysis and risk assessments.
- The agreed recovery time objectives (RTO's).
- The agreed minimum service required.

BCM strategies have four elements. Organisations need to:

- Develop and document an incident response structure.
- Determine how the organisation will recover each critical activity within the RTO and the resources required.
- Determine how relationships with key stakeholders will be managed at the time of disruption.
- Consider those services/activities not defined as critical.

4.3.1 Incident Response Structure

An Incident Response Structure (IRS) is necessary to support all levels of activities that take place during a disruptive event. If no structure exists, there is a danger that emergency response, continuity and eventual recovery plans will be operated independent of each other. This may cause delays, conflicts, incorrect allocation of resources and failure to achieve required levels of continuity.

It is essential the organisation invokes and implements plans in a timely manner as the incident develops in order to maintain control of the situation. In a larger organisation, it is strongly recommended that separation exists between the team that manages the emergency situation, (e.g. fire and evacuation), and the team responsible for ensuring continuity of operations. It is further recommended that, within NHS Scotland, separation exists between the teams that manage medical incidents and continuity of operations.

Procedures must be appropriate to the size and nature of the organisation and set out the basis for determining when a disruption has occurred and how plans will be invoked. Members of an incident response team must have the information, authority and knowledge to be able to assess the situation, confirm

priorities and decide on the appropriate course of action, which may include invoking the appropriate BCM plans.

4.3.2 Selecting the BCM Strategy

The organisation must determine how it will recover each critical service and its essential activities within the RTO and the resources required to do so. In choosing the appropriate option or strategy, the organisation should consider:

- The maximum tolerable period of disruption for each service.
- The cost of implementing the strategy.
- The consequence of inaction.
- The key resources required, e.g. people, premises, technology, information, and supplies.

It is recommended that five scenarios are considered when developing strategies. It is also recommended that organisations only consider the impact of the scenarios rather than the incident that caused the event. The five scenarios are:

- Denial of access to premises.
- Loss of facility
- Shortage of staff.
- Failure of technology.
- Failure of key supplier or partner.
- Failure of utility services.

There are three levels at which strategies can be set:

- Full availability – critical services cannot fail.
- Critical services recovered within the Recovery Time Objectives (RTO)'s at an agreed minimum level.
- Suspend critical services.

It is possible that resumption of a critical service can be phased over a period of time. In such circumstances, it is possible to agree levels of service resumption at fixed points in time, based on the impact of disruption on the organisation [e.g. 25% (minimum level agreed) to be available in 2 hours, 50% available in 2 days, and full service in 1 week].

If the strategy chosen is to suspend certain critical services during a disruptive challenge, it is essential that the stakeholders which have an interest in the critical services that will be suspended are advised that this is the strategy being adopted and why. If the strategy is implemented, communications with the stakeholders is essential to keep them informed as to when the critical service will be restored.

Experience from disruptive incidents has shown that BCM strategies must address the complete loss of IT, standby power, and other essential resources for extended periods. Strategies must therefore be developed for the highest priority services that will enable them to continue under such circumstances.

4.3.3 Relationships with Key Stakeholders

The second stage of the BCM process (Understanding Your Business) identified the organisation's key stakeholders. Stakeholders normally have high expectations of organisations within NHS Scotland. If the organisation is faced with a disruptive challenge, these stakeholders are likely to expect up to date information and be informed of the actions that will or are being taken to maintain critical services and when the organisation will return to normal.

It is therefore essential that a communications strategy is developed to ensure all stakeholders are kept informed. If the organisation has a person or department responsible for public relations then that person/department should be involved in developing this strategy.

4.3.4 Non-Critical Services

It is important to recognise that services or activities which have not been identified as critical must eventually be restored. The period of disruption will have built up a backlog of work that must be 'caught up'. This is referred to as the 'backlog trap' and failure to remove the outstanding work within an acceptable period once the organisation has returned to normal may have serious impacts on customer service, objectives, targets, finance, and reputation.

4.3.5 BCM Strategy Approval

BCM strategies should be agreed and signed off by senior management and, ideally, this should occur before Business Continuity Plan's are developed.

4.4   Stage 4 – Developing and Implementing a BCM Response

Organisations should carry out the key steps in Stages 1-3 before creating a BCP. These steps provide the necessary understanding of the organisation and how it delivers its critical services. If these steps are not carried out in advance, then alternate strategies may not be identified. The resources required may not be properly considered. The plan may not be fit for purpose nor offer the protection and benefits that may have been possible. In contrast, the output from Stages 1-3 help organisations develop realistic and appropriate BCP's.

4.4.1 Developing Plans

Organisations can be disrupted for many reasons. Business continuity planning has traditionally been written on known threats, loss of IT, loss of a building through fire, flooding, etc. In recent times however the UK, including Scotland, has experienced some unexpected disruptions. Such disruptions include a widespread outbreak of foot and mouth disease, extensive disruptions to the rail network, a national shortage of oil based fuels, the loss of water supplies for weeks. In many cases existing plans did not cover these disruptions and the impacts they had on organisations.

It is important that all elements of the organisation are involved in the development of the plans since false assumptions may be made about the ability of other parts of the organisation to respond and meet the needs of the plan.

BCPs should provided answers to basic questions:

- What needs to be done?
- When?
- Where are the alternative resources located?
- Who is involved?
- How is continuity to be achieved?

Organisations may have a number of interconnected plans covering emergency, business continuity, incident, and recovery management. These plans should be appropriate for the organisation. A small organisation, operating from one site may only need a single document that covers incident and continuity management, whilst larger organisations will need integrated corporate, divisional and service unit plans based on a common structure. Such plans must be synchronised to eliminate conflicts and ensure that agreed restoration priorities are achieved. Large organisations should appoint a central BCM team or BCM co-ordinator('s) to undertake this role.

Ownership of the plan(s) must be identified. Large organisations will have plans at various level and business unit managers should own the appropriate operational plans. All plans must be regularly (recommended annually) reviewed and updated, and where necessary, when significant changes occur to the organisation or the environment in which it operates. The responsible owner must undertake this review and the amended plan must then be signed off at a higher level.

Plans must take account of all external arrangements for managing an incident. These include the actions of the emergency services, local authorities and other external agencies including voluntary organisations. If the organisation shares a building then plans must also take into account the emergency and contingency arrangements of the landlord/facilities management company.

The following headings provide guidance on how a BCP might be structured:

- BCM strategy.
- Scope.
- Roles and responsibilities.
- Triggers and activation protocols.
- Invoking the plan.
- Contact details.
- Priorities.
- Communication plan.
- Alternate locations.
- Mutual aid.
- Vital documents and resources.
- Action sheets and check lists.
- Log sheets.
- Staff issues.
- Salvage.
- Return to normal.

Effective continuity plans are written on the basis of recovering the critical services and essential activities of the organisation whatever the cause of the disruption. Plans should provide a framework against which continuity can be achieved.

As the plans are used under challenging and stressful circumstances they should be concise, simple and easy to follow. Plans also need to ensure that the organisation maintains compliance with applicable laws and regulations during the period of their implementation.

Plans will be subject to change and version control and configuration management must be applied. Each copy of the plan must be numbered and a controlled distribution established. Where sensitive information is contained in the plan, it must be given the appropriate level of confidentiality.

4.4.2 Implementing Plans

Implementation of the agreed plan should involve:

- Awareness – Staff holding positions which are named in the plan must be made aware of their role.
- Training – Staff must receive appropriate training to enable them to fulfil their duties and responsibilities. Exercising plans (see section 4.5.1) is one of the principal methods of ensuring that those who will be involved in

managing an incident and effecting continuity are aware of the contents of the plan and their roles.

- Distribution – The organisation should determine how the plans are distributed to staff. Plans and any accompanying documentation must be accessible at all times. They may be held in paper or electronic form.
- Maintenance – The organisation must establish procedures to ensure that plans are maintained and updated as necessary and must make arrangements for control of the plans (see section 4.5.2).
- Communication – Appropriate stakeholders, both internal and external need to be aware that the organisation has plans in place to deal with disruptions. They need to be conscious of what will be done, what services will be available and at what levels. Where appropriate they also need to know what the organisation will not be doing whilst it recovers.
- Duties of External Organisations – External stakeholders, partners and suppliers, who have a role to play in assisting the organisation cope with disruption, need to know their duties and responsibilities to support the organisation's requirements. Since these partners and suppliers may also be impacted by the same disruption it is important that they have plans to maintain their own continuity of service. It is not sufficient to ask a key partner or supplier if a BCP exists or even to have sight of their plan. It is essential that the partner or supplier can demonstrate the effectiveness of the BCM process and that they can meet your organisation's requirements in the event of a disruption.

  BS 25999 has been developed as a certification standard. It will therefore be possible to ask key partners and suppliers to demonstrate compliance with the standard and certification may provide appropriate proof. If a supplier or partner is certified to BS 25999, it is important for, where appropriate, the NHS organisation to determine the scope of their certification and satisfy itself that the partner or supplier can meet the continuity requirements of the NHS organisation.

- Other Activities – Organisations should include BCM requirements into commissioning, procurement and contract management processes.

4.5   Stage 5 – Exercise, Maintenance and Review

4.5.1 Exercise

The Civil Contingencies Act designates geographical NHS Boards in Scotland and the Scottish Ambulance Service as Category 1 Responders. The CCA requires that these Category 1 responders regularly exercise their plans. It is recommended that:

- A regular programme of exercises is established and approved by senior management.

- An exercise of the cascade communications system is carried out on 6 monthly basis.
- A table top exercise is carried out at least annually.
- Where appropriate, a live exercise is carried out at least every 3 years to test the Emergency and Business Continuity Plans.
- Exercises should be organised if there has been significant change to the organisation or to the environment in which it operates.

It is also recommended that those organisations not designated as Category 1 responders also regularly exercise their plans at a level and frequency appropriate to the size and nature of the organisation.

Plans are exercised to ensure that errors and omissions within the plan are identified before the plan is used in reality. (The Chartered Management Institute's research in 2008 found that 87% of those organisations that exercised their BCPs found errors.) If errors or omissions are found while exercising the plan, it is essential that timed based actions are created to rectify these problems.

Exercising also helps to build confidence in team members by clarifying roles and responsibilities, supplying practical training and awareness and providing individuals with valuable experience of responding to an incident.

There are various types of exercise but it is important to:

- Test the systems.
- Test robustness.
- Exercise the plans.
- Rehearse the people.

Exercises must have defined aims and objectives that may include:

- Check everyone understands their role and where their role fits into the overall plan.
- Check the procedures for invoking plans and callout communications work effectively.
- Ensure that the accommodation, equipment, systems and services provided are appropriate and operational.
- Test that the critical services can be recovered within the RTO and to levels required.

It is essential that exercises do not put the organisation at risk by causing disruptions. Exercises must be practical and cost effective, appropriate to the organisation and designed to build confidence in the plan.

The Civil Contingencies Secretariat has provided details of Exercising Good Practice which can be obtained via their website at:

http://www.ukresilience.info/preparedness/ccact/good_practice/exercising.aspx

It is essential that a record of the exercise is kept. To this end, a log of all actions and outcomes must be made during an exercise and this must be reviewed as soon as possible after the event. It is good practice that this review is carried out with the participants so they can express their own views on what went well or otherwise. To assist with this, participants should be asked to maintain their own 'diary of events' throughout the exercise. If independent observers have been used their views should also be included.

A post exercise report should be completed which should include recommendations on changes to the plan. A senior manager of the unit in which the exercise was conducted should sign off the report and the actions to be taken. The process of exercising is set out in the figure below.

Exercising the Business Continuity Plan – The learning cycle

Business Continuity Plan	Exercise	Debrief	Post-Exercise Report	"Lessons Identified" Report

This can be an exercise of part or the whole of the plan

This should be a debrief after each exercise in order to capture the experience of all the participants

The post-exercise report should collate the output of all the debriefs with the post-exercise analysis and of the exercise outcomes

Implement Change	Post –Exercise Report	Audit BCP

Review Plan

Having made changes to the BCP, it is important to review the plan in its entirety before disseminating the "current version"

Approval and acceptance of recommendations by BCM strategic lead within organisation

This report closes the exercise programme and outlines the full outcome of the programme. It makes recommendations for changes to the BCP

The BCP should be audited against the LLR and necessary changes identified

Emergency Preparedness 2005

4.5.2 Maintenance

The purpose of the BCM maintenance process is to ensure the organisation's BCM competence and capability remains effective, fit-for-purpose and up-to-date.

Changes occur on an on-going basis. For example, the organisation itself may change, contact details change, suppliers change, partners change, customers change, and clients change. It is important that processes exist within the organisation to ensure these changes are recorded and the BCPs are adjusted accordingly.

The maintenance programme should also identify any new critical services and their dependent activities and resources that need to be included in the BCM programme. If change is applied, the revised BCP must be subject to version and distribution control within the organisation.

4.5.3 Review

Organisations should review the BCM process at appropriate intervals (annually) to ensure continued suitability, adequacy, and effectiveness. This can be done via an independent audit (either internal or external) of BCM competence and capability to identify actual and potential shortcomings. The organisation should establish, implement and maintain procedures for dealing with such reviews.

A BCM self-assessment process also plays a role in ensuring that an organisation has a robust, effective and fit-for-purpose BCM competence and capability. It can provide the qualitative verification of an organisation's ability to recover from an incident. Self-assessment is regarded as good practice and should be conducted against the organisation's objectives.

6.   Contributors

Thank you to all those people who contributed to the publishing of this operational guidance.

Clairinder Cowan	NHS Greater Glasgow and Clyde
Ian Orr	NHS Fife
Ann McGregor	NHS Fife
Kate Sommerville	National Services Scotland
Brian Steel	SGHD
Philip Wilde	NHS Tayside
John Sharp	QIS

Annex 1

**Good Practice Example –
Suggested Structure of the Overall Business Continuity Plan**

The Business Continuity Plan	
Section A	**Introduction**
Paragraph	
1	Plan Aim
2	Plan Objectives
3	Plan Scope - generic response, specific procedures, current risks
4	Incident trigger definitions – 'Recovery Incident'
5	Recovery Incidents – response objectives
6	Recovery Incidents – control and coordination
7	Recovery Teams – locations, staffing and facilities
8	Recovery Teams – roles and responsibilities
9	Plan review procedure
10	Training objectives
Section B	**Generic Response Plan**
Paragraph	
11	Alerting Phase actions
12	Activation Phase actions
13	Response Phase actions
14	Key contacts
Section C	**Action Cards**
Paragraph	
15	Recovery Team
16	Recovery Manager
17	Recovery Incident Manager
18	Specialist Adviser
19	Recovery Incident Support Team Manager
20	Telephone Operator
21	Log Keeper
Section D	**Corporate Plans And Procedures**
Paragraph	
22	Risk areas for the current programme
23	Other relevant PCT plans and procedures
24	Media Management Guidance Note
Appendix 1	Staff Skills Audit pro forma

.

Annex 2

Good Practice Example – Suggested Incident Check List

Action	Comments/ Action Status
Incident detection and preliminary assessment: • Follow departmental emergency response procedures • Conduct a preliminary assessment, if it can be done safely. No recovery activities should be undertaken if personnel are	
Activate incident management team: • Notify Incident Management Team Members • Provide a description of the event • Request that they assemble at the Control Room • Activate the Control Room	
Evaluate incident impact: • Determine if the severity of the impact requires implementation of the recovery plan • Determine recovery objectives including, priorities, recovery	
Activate recovery plan: • Notify recovery team leaders and members • Brief recovery team leaders and alternates regarding, priorities, strategies, action plans, assignments, reporting and	
Track incident status and recovery progress: • Open and commence log of events/decisions (see section 18 of DRP if held) • Conduct periodic debriefing sessions with recovery teams to	
Reallocate and/or provide resources:	

Annex 2 Continued – Key Contact Details

Name	Telephone Number	Extension	Mobile Number

Annex 3

Good Practice Example – Structure for a Business Impact Analysis

Sheet 1 : Simplified Business Impact Analysis (BIA)

1.   List your organisations <u>Key Functions</u> in priority order.

Key Functions (Priority Order)
1.
2.
3.
4.
5.

2.   Using the guidance set out below undertake a Business Impact Analysis of your department, filling in your answers to the following questions on the blank BIA Pro-forma (Sheet 2) under the relevant headings :

PEOPLE	PREMISES	PROCESSES	PROVIDERS	PROFILE
Key Staff: What staff do you require to carry out your key functions?	**Buildings:** What locations do your department's key functions operate from? (Primary site, alternative premises)	**IT:** What IT is essential to carry out your key functions?	**Reciprocal Arrangements:** Do you have any reciprocal agreements with other organisations?	**Reputation:** Who are your key stakeholders?
Skills/ Expertise/ Training: What skills/ level of expertise is required to undertake key functions?	**Facilities:** What facilities are essential to carry out your key functions?	**Documentation:** What documentation/ records are essential to carry out your key functions, and how are these stored?	**Contractors/ External Providers:** Do you tender critical services out to another organisation, to whom and for what?	**Legal Considerations:** What are your legal, statutory and regulatory requirements?
Minimum Staffing Levels: What is the minimum staffing level with which you could provide some sort of service?	**Equipment / Resources:** What equipment / resources are required to carry out your key functions?	**Systems & Communications** What systems and means of communication are required to carry out your key functions?	**Suppliers:** Who are your priority suppliers and whom do you depend on to undertake your key functions?	**Vulnerable Groups:** Which vulnerable groups might be affected by failing to carry out key functions?

Sheet 2 : BIA Pro-Forma For Your Department (Function)

PEOPLE	PREMISES	PROCESSES	PROVIDERS	PROFILE
Key Staff:	Buildings:	IT:	Reciprocal Arrangements:	Reputation:
Skills/ Expertise/ Training:	Facilities:	Documentation :	Contractors/ External Providers:	Legal Considerations:
Minimum Staffing Levels:	Equipment/ Resources:	Systems & Communications	Suppliers:	Vulnerable Groups:

Sheet 3 : Considerations For Increasing Your Organisations Resilience

People	Premises	Processes	Providers	Profile
Key Staff: Can staff be contacted out of hours? Could extra capacity be built into your staffing to assist you in coping during an incident?	**Buildings:** Could you operate from more than one premise? Could you relocate operations in the event of a premise being lost or if access to the premise was denied?	**IT:** Is data backed-up and are back-ups kept off site? Do you have any disaster recovery arrangements in place?	**Reciprocal Arrangements:** Do you have agreements with other organisations regarding staffing, use of facilities in the event of an incident?	**Reputational Damage:** How could reputational damage to your organisation be reduced? How could you provide information to staff and stakeholders in an emergency (e.g. press release)?
Skills / Expertise / Training: Could staff be trained in other roles? Could other members of staff undertake other non-specialist roles, in the event of an incident.	**Facilities:** Are any of your facilities multi-purpose? Are alternative facilities available in the event of an incident?	**Documentation:** Is essential documentation stored securely (e.g. fire proof safe, backed-up)? Do you keep copies of essential documentation elsewhere?	**Contractors / External Providers:** Do you know of alternative contractors or are you reliant on a single contractor? Do your contractors have contingency plans in place? Could contractors be contacted in the event of an incident?	**Legal Considerations:** Do you have systems to log decisions; actions; and costs, in the event of an incident?
Minimum Staffing Levels : What is the minimal staffing level to continue to deliver your key functions at an acceptable level? What measures could be taken to minimise impacts of staff shortfalls?	**Equipment / Resources :** Could alternative equipment / resources be acquired in the event of an incident / disruption? Could key equipment be replicated or do manual procedures exist?	**Systems & Communications** Are your systems flexible? Do you have alternative systems in place (manual processes)? What alternative means of communication exist?	**Suppliers :** Do you know of suitable alternative suppliers? Could key suppliers be contacted in an emergency?	**Vulnerable Groups :** How could vulnerable groups be contacted / accommodated in the event of an incident?

Sheet 4 : Using Business Impact Analysis To Build A Plan

BIA Identifies your requirements for continuing your key functions	BUSINESS CONTINUITY PLAN Documents how your requirements identified in the BIA can be achieved	
PEOPLE	• Key Staff • Key Skills • Expertise/competence required • Minimum staffing levels required to continue/recover key functions	• Notification/invocation procedure/protocol • Management structure for dealing with an incident • Information and advice to staff (response procedures) • Key staff / contact list (including out of hours details) • Multi skill training in key areas • Reciprocal Arrangements to cover staff short falls • Home working • Staff welfare issues
PREMISES	• Key facilities • Key Equipment • Key Resources • Specialist Equipment • Security/restrictions • Alternative sites • Alternative facilities	• Loss/damage assessment • Site security • Relocation arrangements/protocol • Inventories of equipment/resources and details of how to recover these • Salvage, site clearance and cleaning arrangements
PROCESSES	• Key processes • Critical periods • Key IT systems/applications • Key documentation/data • Record keeping requirements • Key communication requirements	• Action cards for recovery of key processes • Checklists • Copies/Back-ups/safe storage (recovery procedure) • Contingency procurement arrangements • Documented manual procedures • Data recovery procedures
PROVIDERS	• Key dependencies (supply and receipt) • Key suppliers • Key contractors/service providers/ suppliers • Reciprocal arrangements in place with other organisations	• Contact details for key providers/ contractors/suppliers/support services • Alternative suppliers (required for key functions) • Alternative providers (required for key functions) • Alternative contractors (required for key functions) • Resilience capability of suppliers/providers /contractors to business disruption • Third party business continuity arrangements
PROFILE	• Key stakeholders • Legal/statutory/regulatory requirements • Vulnerable groups	• Communication strategy/plan /procedures • Stakeholder liaison (regulator, clients, unions) • Media liaison • Public information/advice • Notification of at risk groups / alternative care arrangements

Annex 4 – Risk Analysis Matrices

Table 1 – Impact/Consequence Definitions

Descriptor	Negligible	Minor	Moderate	Major	Extreme
Patient experience	Reduced quality of patient experience/clinical outcome not directly related to delivery of clinical care	Unsatisfactory patient experience/clinical outcome directly related to care provision – readily resolvable	Unsatisfactory patient experience/clinical outcome: short term effects – expect recovery <1 week	Unsatisfactory patient experience/clinical outcome; long term effects – expect recovery >1 week	Unsatisfactory patient experience/clinical outcome; continued ongoing long term effects
Objectives/ Project	Barely noticeable reduction in scope, quality or schedule	Minor reduction in scope, quality or schedule	Reduction in scope or quality of project, project objectives or schedule	Significant project over-run	Inability to meet the project objectives; reputation of the organisation seriously damaged.
Injury (physical and psychological) to patient/visitor/ staff	Adverse event leading to minor injury not requiring first aid	Minor injury or illness, first aid treatment required	Agency reportable, e.g. Police (violent and aggressive acts). Significant injury requiring medical treatment and/or counselling	Major injuries/long term incapacity or disability (loss of limb) requiring medical treatment and/or counselling	Incident leading to death or major permanent incapacity
Complaints claims	Locally resolved verbal complaint	Justified written complaint peripheral to clinical care	Below excess claim. Justified complaint involving lack of appropriate care.	Claim above excess level. Multiple justified complaints.	Multiple claims or single major claim. Complex justified complaint
Service/business interruption	Interruption in a service which does not impact on the delivery of patient care or the ability to continue to provide service.	Short term disruption to service with minor impact on patient care.	Some disruption in service with unacceptable impact on patient care. Temporary loss of ability to provide service.	Sustained loss of service which has serious impact on delivery of patient care resulting in major contingency plans being invoked.	Permanent loss of core services or facility. Disruption to facility leading to significant "knock on" effect.
Staffing and competence	Short term low staffing level temporarily reduces service quality (<1 day).	Ongoing low staffing level reduces service quality. **Minor error** due to ineffective training/implementation of training.	Late delivery of key objective/service due to lack of staff. **Moderate error** due to ineffective training/implementation of training. Ongoing problems with staffing levels.	Uncertain delivery of key objective/service due to lack of staff. **Major error** due to ineffective training/implementation of training.	Non-delivery of key objective/service due to lack of staff. Loss of key staff. **Critical error** due to ineffective training/implementation of training.
Financial (including damage/loss/ fraud)	Negligible organisational/personal financial loss (£<1k). (**NB** please adjust for context).	Minor organisational/personal financial loss (£1 – 10k).	Significant organisational/personal financial loss (£10 – 100k).	Major organisational/personal financial loss (£100k – 0 1m)	Severe organisational/personal financial loss (> £1m).

Inspection/audit	Small number of recommendations which focus on minor quality improvement issues.	Recommendations made which can be addressed by low level of management action.	Challenging recommendations that can be addressed with appropriate action plan.	Enforcement action. Low rating. Critical report.	Prosecution. Zero rating. Severely critical report.
Adverse publicity/ reputation	Rumours, no media coverage. Little effect on staff morale.	Local media coverage – short term. Some public embarrassment. Minor effect on staff morale/public attitudes.	Local media – long term adverse publicity. Significant effect on staff morale and public perception of the organisation.	National media –adverse publicity, <3 days. Public confidence in the organisation undermined. Use of services affected.	National/international media – adverse publicity >3 days. MSP/MP concern (Questions in Parliament). Court enforcement. Public Inquiry/FAI.

Table 2 – Likelihood Definitions

Descriptor	Rare	Unlikely	Possible	Likely	Almost Certain
Probability	Can't believe this event would happen – will only happen in exceptional circumstances.	Not expected to happen, but definite potential exists – unlikely to occur.	May occur occasionally, has happened before on occasions – reasonable chance of occurring.	Strong possibility that this could occur – likely to occur.	This is expected to occur frequently/in most circumstances – more likely to occur than not.

Table 3 – Risk Matrix

Likelihood	Consequence/Impact				
	Negligible 1	Minor 2	Moderate 3	Major 4	Extreme 5
Almost Certain 5	Medium 5	High 10	High 15	V. High 20	V. High 25
Likely 4	Medium 4	Medium 8	High 12	High 16	V. High 20
Possible 3	Low 3	Medium 6	Medium 9	High 12	High 15
Unlikely 2	Low 2	Medium 4	Medium 6	Medium 8	High 10
Rare 1	Low 1	Low 2	Low 3	Medium 4	Medium 5

Low Risk (1 – 3)   Accept

Moderate Risk (4 – 6)   Control

High Risk (8 – 12)   Plan

Extreme Risk (15 – 25)   Reduce

Annex 5

Good Practice Example – Suggested BCM Audit Checklist

This suggested BCM Audit checklist for use by NHS organisations was originally produced by John Sharp, BCM Consultant Kiln House Associates, and the Cabinet Office Civil Contingencies Secretariat

BCM Programme		
Key Issues	Example Evidence	Rating
Responsibility for BCM issues is clearly defined within the organisation at the corporate management level.	Named executive director accountable for BCM policy and implementation Reports to senior management groups	1 – 5
BCM Manager or Co-ordinator appointed	Named individual in post responsible for implementing and maintaining the BCM programme	1 – 5
BCM is formalized through the organisations policy and procedures	A BCM policy exists The BCM policy is published internally and externally	1 – 5
Responsibility for business continuity issues is well embedded within individual services or management units	BCM is included in job descriptions and skill sets of service and support managers. BCM responsibilities enforced by inclusion in organisation's appraisal, reward and recognition policies.	1 – 5
Responsibility for business continuity issues is well embedded within the organisation.	Evidenced through minutes of meetings and reports. Induction programmes include awareness of BCM. There is a programme in place raising awareness throughout the organisation and its key stakeholders. Feedback mechanisms exist whereby functional managers and staff can flag up BCM issues	1 – 5
Assurance of organisation's BCM capability	KPIs set for BCM implementation and maintenance. BCM responsibilities reviewed by the organisations audit process.	1 – 5

(Continued)

Understanding the Organisation

Key Issues	Example Evidence	Rating
Identification of the organisation's objectives, stakeholder obligations, statutory duties and environment in which the organisation operates	Analysis of stakeholder obligations and expectations. Listing of statutory duties	1 – 5
Critical services and products delivered by and on behalf of the organisation have been identified and have been agreed by the executive board	Documented procedures for identifying and reviewing critical services and products. Executive board minutes confirming critical services and products.	1 – 5
Critical functions, processes and supporting resources, within and without the organisation, that are needed to delivery the critical services and products identified.	Documentation detailing critical functions, processes and supporting resources. Mapping of critical suppliers and partners	1 – 5
Risk assessment has been used on the critical activities and supporting resources to focus effort on the areas of greatest need	Documented procedures to review and rank risk. Identification of 'single points of failure'	1 – 5
Countermeasures exist to minimise risks that have been identified, including measures to combat potential loss of information.	Documented evidence of risk mitigation covering people, systems, information, premises and equipment and suppliers..	1 – 5
Identification of the impact over time on the organisation and its stakeholders of the loss of any key service or product	A structured business impact analysis (BIA) process exists for the organisation that prioritises critical services and products. A documented BIA that covers the critical services and products of the organisation. Executive board minutes confirming BIA.	1 – 5

Determining BC Strategies

Key Issues	Example Evidence	Rating
Development of appropriate strategies to limit, over time, the impact of the loss of critical services and products on the organisation and its stakeholders	Documented strategies to support each key service and product. Strategies cover: people, premises, technology, information, supplies and stakeholders. Strategies take account of other Category 1 responder's actions, including those undertaken in an emergency situation. Executive board minutes confirming strategy selection and their required resource allocations.	1 – 5
Development of strategies to minimise supplier disruption.	Alternative suppliers identified. Procurement policies for key supplies that require BCM to be incorporated into supply contracts. Evidence of BCM included in supply contracts.	1 – 5

(Continued)

Developing and Implementing a BCM Response

Key Issues	Example Evidence	Rating
Generic business continuity plans (BCPs) are developed which are flexible enough to maintain continuity of critical services and products through a range of disruptive events	Structure and procedures for developing BCM plans. Reports. Meeting minutes Plans are clear, unambiguous and easy to use. Documented evidence of consultation with relevant staff in functional units and incorporation of feedback during plan development. BCM plans identify objectives, personnel involved, and command and control arrangements **BCPs contain references to other sources of relevant information, advice and other documentation.**	1 – 5
A clear procedure exists for invoking the BCPs and delivering the response	Documented invocation and response procedures Key staff are identified in plans. Call out lists for BCM team members.	1 – 5
BCPs have clear ownership and are signed off at the appropriate level.	**It is clear who is responsible for ensuring that each section/department or site has a BCP.** All BCPs are signed off by plan owners.	1 – 5
Appointment of a BCM team that is trained to deliver the BCPs	**Details of BCM team members.** **Training programme for BCM team members.** **Training record for BCM team members.**	1 – 5
A clear procedure exists that ensures internal and external stakeholders are aware of what actions the organisation's will take if BCPs are activated	A communications policy document. Letters, emails, circulars, meeting minutes, internet and intranet pages which raise awareness of BCPs.	1 – 5
Ensuring communications with stakeholders at the time of disruption to critical services and products	BCPs contain arrangements for communicating with clients, customers, staff, stakeholders, partners, and the media. BCPs linked to Communication plans.	1 – 5
Ensuring latest BCPs and supporting materials are always available.	Copies of plans and essential equipment/ documents (in electronic or hard copy) are easily available on and off- site. All plans are subject to document and version control processes.	1 – 5
BCPs linked to other event plans within and without the organisation.	Links to emergency, recovery, major incident, communication plans, etc. are documented.	1 – 5

(BCM Audit Checklist Continued)

Exercising

Key Issues	Example Evidence	Rating
Ensuring there is a balanced programme of exercise types which validates the full range of BCM capabilities	Records of regularly tested contact arrangements and exercises Planned exercises /test schedules.	1 – 5
Exercise programmes have clear objectives	Exercise scenarios	1 – 5
Ensuring there is a documented process for capturing and taking forward the lessons identified	Notes of exercise debriefs, 'lessons learnt' reports. Exercise review report to relevant management team. Action plans. Review of actions at plan preparation/review meetings. Evidence that the lessons learnt from exercises have been incorporated into BCPs.	1 – 5

Maintaining

Key Issues	Example Evidence	Rating
Ensuring that the BCPs are kept up to date	There is an established and documented BCP review process. BCP review is built into the business planning cycle. Notes from review meetings. Issue of version controlled updates and acknowledgement systems for recipients	1 – 5
Ensuring that when major changes to the organisation, the environment in which it operates or threat levels change the organisation's BCPs are reviewed and modified if appropriate.	There is a mechanism to identify trigger BCP review points. Notes from review meetings. Actions plans Review of actions at plan preparation/review meetings	1 – 5

Reviewing

Key Issues	Example Evidence	Rating
A clear mechanism is in place for measuring the effectiveness of BCM arrangements	BCM review programme Self assessment reports Internal audit reports Benchmarking against standards (e.g. BS 25999) and guidelines External reviews by peers from other services, partner authorities, etc.	1 – 5
Ensuring that the review process drives improvement by identifying lessons, and appropriate action is taken	Review reports to relevant management team. Action plans. Review of actions at BCM review meetings. Evidence that the lessons identified from reviews have been incorporated into the organisations BCM processes.	1 – 5