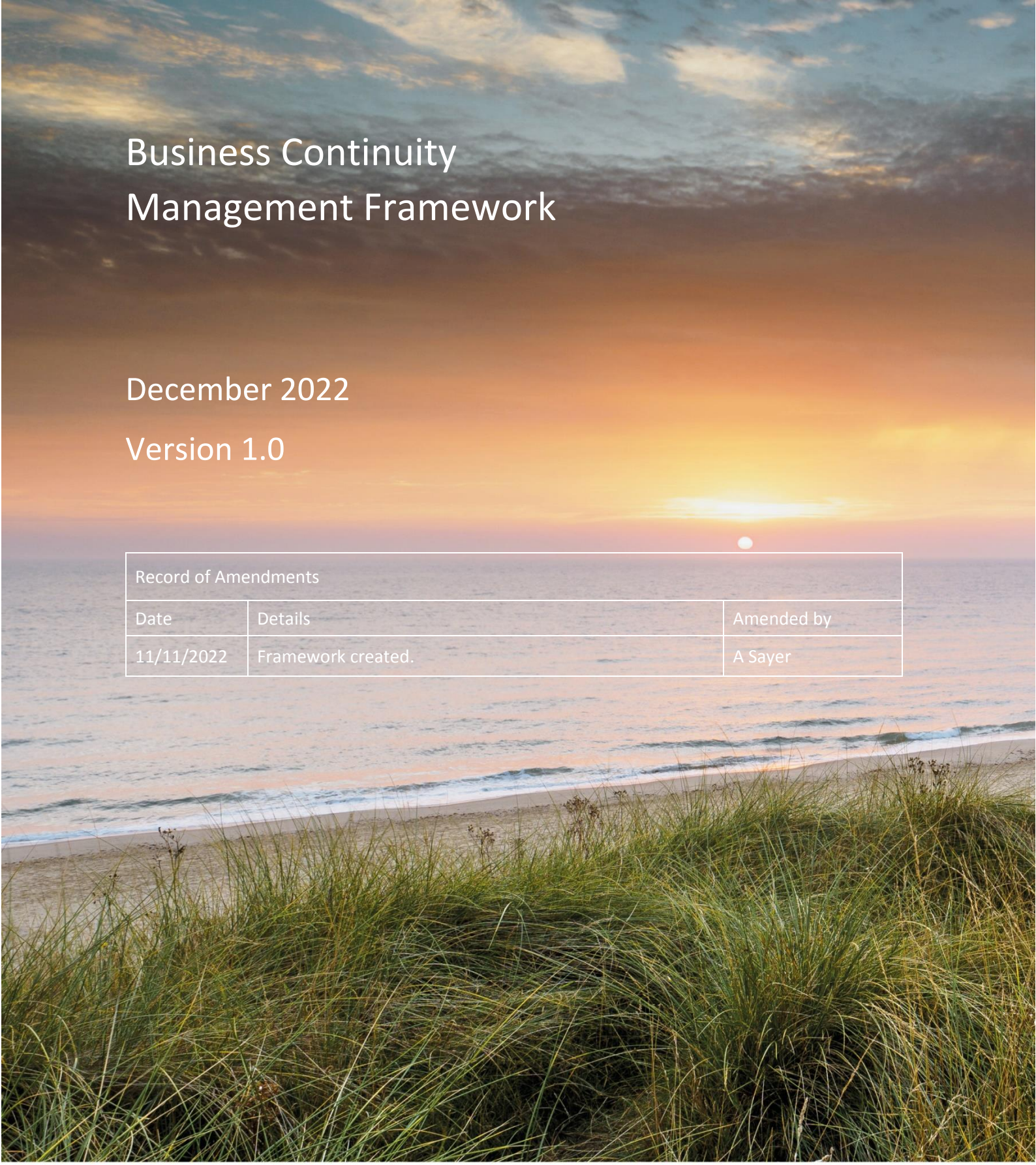
Business Continuity Management Framework

December 2022

Version 1.0

Record of Amendments		
Date	Details	Amended by
11/11/2022	Framework created.	A Sayer



NORTH NORFOLK DISTRICT COUNCIL

Contents

Foreword

The residents and businesses of North Norfolk expect the services provided by the Council to be delivered effectively and consistently. It is important to ensure there are procedures in place to enable the Council to continue to provide services in the face of a range of potential disruptions.

All departments must ensure they have effective Business Continuity arrangements in place not just because it is good management practice but also because it is a requirement of the Civil Contingencies Act 2004.

North Norfolk District Council's Business Continuity Plans identify the procedures and resources required to prepare for and respond to disruptions that may affect its ability to provide essential services.

This Business Continuity Framework establishes the basis on which the Corporate Business Continuity Plan and individual Business Continuity Plans are developed, implemented and reviewed.

Signed:	Signed:
Steve Blatch	Tim Adams
Chief Executive	Leader of the Council
North Norfolk District Council	North Norfolk District Council

Context

Business Continuity is both good management practice and a statutory requirement for local authorities under the Civil Contingencies Act (CCA) 2004.

Business Continuity Management (BCM) is a process which identifies and prepares for potential disruptions and seeks to ensure that steps are taken to increase the resilience of "prioritised activities" in advance of a disruption, enabling the Council to maintain delivery of essential functions. BCM is not a one-off project; it is an ongoing activity that should be embedded into the core of the organisation.

This framework explains what Business Continuity Management is, how it is adopted at North Norfolk District Council, and establishes the basis within which the Corporate Business Continuity Plan and service Business Continuity Plans are developed, implemented and reviewed, so that the Council meets its duties in legislation and complies with best practice.

The short-term objective of BCM is to ensure that during a business disruption critical services continue uninterrupted. The longer-term objective of BCM is to ensure that the Council can resume normal services as quickly as possible in the aftermath of any disruption / emergency event.

The framework should be read in conjunction with the Business Continuity Policy and the Corporate Business Continuity Plan.

1. Aim and Objectives

The aim of the Business Continuity Management Framework is to develop a resilient Council. The objectives are to:

- Ensure, where practicable, the Council can continue to deliver its Key Activities in the event of a disruption
- Identify areas of vulnerability in Council services so that effective mitigation measures can be put in place
- Prioritise corporate functions and responsibilities which are essential for the Council to deliver so that overall priorities for recovery are clear
- Describe contingency arrangements to respond to serious disruption, allocating resources and priorities for action to recover critical functions and prepare for return to normal working as quickly as possible
- Describe the communication strategy to ensure information is disseminated effectively during a service disruption
- Ensure all Council service areas are involved in the preparation of service level Business Continuity Plans, to inform the Corporate Business Continuity Plan and so that there is an effective and consistent response to service continuity
- Provide a basis for cost benefit analysis based on risk appetite to determine which specific risk prevention and mitigation actions will be adopted corporately and within service areas

- Build on work already in place for risk management, ensuring existing processes are integrated into the BCM Framework and BC Plans that this is incorporated appropriately into BC plans
- Develop a process to monitor, review, update and validate the Corporate BC Plan and Service BC Plans
- Deliver training and awareness programmes for staff, Elected Members, suppliers, partners and contractors
- Carry out regular tests of plans to validate and further develop BC arrangements
- Embed BCM throughout the organisation.

2. An effective BCM programme

The elements comprising Business Continuity Management are set out in the Business Continuity Institute's Good Practice Guidelines, 2018. The Business Continuity Lifecycle is shown below:

2.1. Policy and Programme Management

Legislation and Guidance

As a defined Category 1 responder under the Civil Contingencies Act 2004, NNDC must demonstrate that it meets the requirements for Business Continuity as detailed within this legislation. In addition, NNDC must ensure that it complies with the Business Continuity Good Practice Guidelines (GPG) 2018.

Governance Risk and Audit Committee (GRAC)

This group agrees, supports and guides the BCM work across the authority. This group is responsible for ensuring the CLT is kept informed of progress toward embedding BCM practices.

Business Continuity Policy

The policy outlines the approach to BCM within NNDC. The policy describes the governance arrangements which have been agreed by the Corporate Leadership Team and Members.

Related roles and responsibilities are as follows:

Chief Executive

- To be a positive champion for BCM across the Council
- Ultimately responsible for the Council's overall BCM arrangements

Corporate Leadership Team (CLT)

- Has overall responsibility for NNDC's services and their continuity
- Maintains an overview of the work associated with Business Continuity, with one member of the Team having overarching responsibility
- Enables the embedding of BCM across the Council
- Ensures that this framework and associated plans are implemented and resourced appropriately
- Supports business continuity planning activity

Resilience Manager (Civil Contingencies Team)

- Responsible for coordinating the BCM programme, supporting the implementation of the BCM process and ensuring information is collated for GRAC
- Makes available best practice tools (such as templates) to support Service Managers
- Supports and advises service areas
- Identifies training needs and supports delivery
- Undertakes basic Quality Control – reviews BIAs and service BC Plans
- Supports the facilitation of testing and exercising of the Council's BCPs when requested by the Chief Executive, Directors or Service Managers
- Following an incident, facilitates debriefing session(s) if required
- Leads on the council's statutory duty to promote BCM in the community

Service Managers

- Lead on Business Continuity arrangements within their service area
- Ensure the BC Plan for their service area remains current
- Review the Business Impact Analysis for their service area every two years
- Attend training commensurate with their role
- Identify staff from their teams that have a role to play in any recovery for suitable training
- Implement the agreed arrangements in the event of a disruption
- Advise the Resilience Manager of any changes that may impact on the contents or procedures outlined in this policy

All Staff

- Familiarise themselves with BC arrangements within their area
- Attend training commensurate with their role
- Engage with testing and exercising

2.2. Analysis

It is vital to understand the critical activities of NNDC. These are the Key Activities which must be maintained as a priority during an incident. A Business Impact Analysis (BIA) must be completed for all services delivered by the authority.

The purpose of the BIA is to:

- List the organisation's services and the Key Activities supporting these
- Document the impacts over time that would result from loss or disruption of a service/activity, aligned with the Council's Risk Management Policy and Framework
- Identify when a disruption would cause significant adverse impacts on services
- Determine priorities for continuity and recovery
- Identify the dependencies and resources that are required to achieve service expectations
- Prevent incidents from occurring by taking preventative steps in advance of, or whilst developing, a BC plan.

Key Activities which have an impact score of 4 ('Major') or 5 ('Extreme') within a week are considered 'Critical activities' for NNDC. Mitigations are considered in more detail for these activities.

Critical activities and non-critical activities have been reviewed and agreed by the Corporate Leadership Team. Critical activities are documented in the Corporate Business Continuity Plan. Departments have considered risks to their critical activities. Many of these risks have already been captured and are being managed on the Corporate Risk Register.

To implement this we will:

- Complete the Business Impact Analysis for each service area every 2 years, this must be consistently completed across the organisation
- Complete the BIA at a high level, capturing activities broadly; avoiding operational detail will minimise the resource required and ensure activities can be prioritised consistently across the organisation.
- Agree NNDC-Critical activities and non-critical activities through CLT
- Demonstrate that departments have taken steps to increase the resilience of their service/critical activities
- Ensure steps are taken to connect the Risk Management process and Business Continuity process actively, to remove duplication
- Ensure all services will have agreed Recovery Timescales assigned to them.

2.3. Design

Once critical activities have been agreed and have recovery timescales assigned to them, it is important that services consider how these timescales may be met in the event of an incident.

There are different solutions to help ensure continuity of services, those considered by NNDC are categorised as follows:

- People (skills and knowledge)
- Premises (buildings and facilities)
- Resources (IT, information, equipment, materials, etc.)
- Suppliers (products and services supplied by third parties)

The table below details the actions required to ensure activities are more resilient and the level of disruption experienced in an incident will be minimised when these are embedded.

People • Ensure that succession planning is considered appropriately. • Ensure key processes are documented and process maps written, enabling others who are less familiar with tasks to complete or support activities. • Ensure critical skills for prioritised activities are documented. • Ensure there is a process to support the transfer of knowledge for those joining the authority, leaving the authority and transferring to new departments. • Ensure staff are trained appropriately and are aware of their BC roles and responsibilities. Ensure there is clarity on out-of-hours working arrangements and remuneration during BC disruptions. • Ensure managers share the contents of their Business Continuity plan with their team. • Ensure managers keep a copy of their plan(s) securely (which is not dependent on a network connection; for example print a hard copy and keep it securely offsite). • Consider how critical activities would be maintained and which services would be potentially suspended in the event of having 25% + staff off sick e.g. as a result of Pandemic Influenza • Ensure managers have arrangements to multi-train/skill all appropriate staff, so that activities are not reliant on a small number of individuals. • Ensure staff skills not utilised within their existing roles are captured to allow maximum flexibility or redeployment. • Test staff contact numbers regularly. • Ensure contact details in Business Continuity plans are reviewed every 6 months. • Encourage staff to take advantage of the NNDC Well Being programme which includes developing personal resilience.
Premises • Ensure that Fakenham Connect is available as a Work Area Recovery site for critical services. • Assess other suitable sites for Work Area Recovery purposes in the event of the Cromer office being inaccessible. • Ensure an assessment is made on the resilience of existing and future premises.

- Ensure evacuation procedures are in place which minimise disruption and support recovery.
- Develop plans for key premises.

Information and Technology

- IT Services must have suitable BC plans in place that link with service/departmental BC plans
- Service BC plans with Critical Activities must include their IT requirements/software to enable IT Services to prioritise systems recovery
- IT Services to develop and maintain a Disaster Recovery plan including arrangements for Cyber attack and National Power Outage/rolling power outage.
- Maintain sufficient planned capacity for remote working – with critical services having priority.
- Ensure IT Continuity/Disaster Recovery arrangements and plans are developed and exercised.
- Ensure staff follow all relevant IT guidelines i.e. not saving key documents in locations colleagues cannot access.
- Ensure IT work is developed in accordance with requirements of the agreed critical activities.
- Ensure consideration is given to Business Continuity arrangements within ICT projects.
- Copies of vital records and essential documentation should be kept separate from originals, possibly at a work area recovery location.
- Where services can continue without IT, “manual workarounds” should be documented.
- IT Services should include Business Continuity within their ICT contracts and involve the Civil Contingencies Team within the process.
- IT Services should have a clearly documented process for managing ICT disruptions affecting external clients and ensuring effective communications with clients.
- IT Services will provide ongoing briefings to CLT to ensure they are aware of the risks to business continuity of any new technology introduced.
- Ensure that guidelines exist on the use of personal devices in an incident.e.g. using WhatsApp on personal devices.

Suppliers

- As NNDC is a commissioning organisation BC must be an important part of all procurement documents and procedures.
- Critical suppliers (suppliers supporting our critical activities) must have Business Continuity arrangements, including documented plans.
- Business Continuity must be referenced within the contractual process as well as in the contract itself.
- Business Continuity must be actively promoted to the supply chain.
- Business Continuity must be included as part of the QA and review process of provider’s arrangements.
- NNDC must review a sample of providers/suppliers BC arrangements each year.

General

- All departments to assess the risks which could impact their critical activities and ensure that these, together with mitigation measures, have been documented appropriately on risk registers.

To implement this we will:

- Review the above actions for increasing service resilience annually with the service managers
- Liaise with Directors and Assistant Directors to ensure that appropriate action is being taken.

2.4. Implementation

As a result of the Business Impact Analysis (BIA), and the development of the above actions to enable continuity and support recovery, BC plans must be created and developed/updated. The term "business continuity plan" is defined as "documented procedures that guide organisations to respond, recover, resume, and restore to a pre-defined level of operation following disruption."

Documents include:

- A Corporate Business Continuity Plan to guide the Council in response to an incident affecting the council's ability to deliver its services, each service is to be responsible for creating its own BC plan. The Corporate BC Plan is to be reviewed annually, updated every two years and be tested at least once every three years.
- Each service to be responsible for maintaining their own BC plans and procedures in accordance with the Business Impact Analysis and corporate policies and procedures. The BC Plans to be reviewed annually and the BIAs to be reviewed every two years
- The maintenance of other suitable documentation, processes and procedures to assist the Council in meeting the requirements of the Civil Contingencies Act 2004

Business continuity plans should be held securely online and in hard copy securely offsite, so that managers have access to a copy in the event of losing access to IT. Consideration should be given to having plans available on Resilience Direct as a backup (facilitated through the Civil Contingencies Team).

Service managers should share the contents of the BC plan with the team, with due regard to the General Data Protection Regulation, so the team is aware of the plan and requirements in the response to an incident.

Critical or prioritised activities have a shorter recovery timescale or "Recovery Time Objective" than other activities and so will be given priority during service disruptions or major incidents. It is imperative that there are comprehensive Business Continuity plans in place for all critical activities. Activities which are not critical may have simplified BC plans.

The content of plans is shown below.

Corporate BC Plan
The Corporate Business Continuity Plan identifies recovery objectives, the structure for implementation, mitigation measures and the communication process to keep staff, members, partners and the public informed. It includes:

- Critical activities as agreed by CLT
- Invocation procedures
- IT system priorities
- Work area recovery strategy and arrangements
- Key contacts
- Roles and Responsibilities
- Incident categories

- Incident action checklists

Service/Team plans
Service/Team Plans draw on the recovery objectives from the Business Impact Analysis and set out the team's response during a disruption. They include:

- Team priorities
- Invocation procedures
- Numbers of staff required and when
- Resources required and when – including IT systems and software. This must be agreed through the BIA and recovery timescales.
- Key requirements such as vital data or equipment
- Incident action checklists
- Key contacts

Note: Teams undertaking NNDC Critical activities must have comprehensive Business Continuity plans.

To implement this we will:

- Review the Business Continuity Framework every two years
- Review the Corporate and service BC plans once a year
- Ensure all teams undertaking corporately agreed critical activities have comprehensive BC plans.

2.5 Validation

Validation is achieved through a combination of the following three activities:

- **Exercising –** a process to train for, test, assess, practice and improve the business continuity capability of the organisation
- **Maintenance** - a process to ensure that the organisation's business continuity arrangements and plans are kept relevant, up-to-date, and operationally ready to respond
- **Review** - a process for assessing the suitability, adequacy and effectiveness of the business continuity programme and identifying opportunities for improvement

To meet the requirements of best practice as set out in the Good Practice Guidelines (GPG) service plans must be exercised (tested) at least once a year. In the event of a service having several live incidents, it may be acceptable not to run an exercise that year, provided that the incident is fully debriefed, and any necessary changes are made to the plan.

Following disruption to 'business as usual' a debrief must always take place with lessons identified being captured. The debrief can be completed by the team itself or in collaboration with the Civil Contingencies Team. It is important for BC arrangements to be updated and for plans and procedures to be kept up-to-date as a result of these actions.

Audits should be completed regularly to check plans are fit for purpose and are being updated and are kept current.

To implement this we will:

- Establish an exercise and training programme
- Ensure the Corporate BC plan is validated annually and that senior managers are involved and briefed
- Complete a debrief after every incident and cascade the results to those involved. For a significant incident a face to face debrief will be organised, for a minor incident an email asking for feedback may be more appropriate
- Ensure departments have an annual programme of exercises
- Ensure each plan is exercised annually.

2.6 Embedding Business Continuity

To be successful, BCM must become part of the culture of NNDC. The culture plays an important role in the effectiveness of embedding the business continuity programme and the overall level of organisational resilience.

Awareness-raising events such as training, workshops, exercises and regular management briefings will help to ensure that staff are aware of why BCM is important to NNDC.

To embed Business Continuity into the organisation we will;

- Consider the willingness of individuals to undertake BC-related tasks, such as maintaining plans, in addition to their normal roles
- Share best practice information within departments
- Implement a programme of training at different levels within the organisation
- Ensure exercises are being completed at appropriate intervals
- Highlight concerns and non-compliance to CLT
- Agree a programme of communications to NNDC staff with the Communications Team to develop awareness and understanding
- Establish levels of awareness of Business Continuity within the organisation and then review this on an annual basis.

3. Monitoring and review of the BCM Framework

- The BCM Framework will be reviewed every two years, when there are significant structural re-organisations, or when new duties or responsibilities are taken on. It is the responsibility of the Corporate Leadership Team, Assistant Directors and Service Managers to notify the Resilience Manager of any significant changes that occur between these updates.
- Periodically and in line with the Council's auditing policy, the Corporate BC Plan and service BC Plans may be audited by either the internal audit team or external auditors appointed by the Council. The Resilience Manage will complete audits on a minimum of 20% of Business Continuity plans each year

The Resilience Manager will:

- Follow the work plan which includes checking that the activities undertaken are in line with the BCM Framework
- Produce an annual report for review by the Governance Risk and Audit Committee which will outline the achievements and challenges of the programme for each year. The report will be made available and circulated to the Corporate Leadership Team

- Ensure service BC plans are reviewed by the plan owners every 12 months, with a 6-monthly check on all contacts
- Produce a BCM progress report for CLT/GRAC once a year or when there is an organisational requirement

The Governance, Risk and Audit Committee will:

- Monitor risks associated with and the effectiveness of Business Continuity Management (BCM) arrangements
- Review the BC Framework and associated documentation

Cabinet will:

- Set the strategic direction of Business Continuity Management across the Council
- Approve the Business Continuity Management Framework

4. Related policies and plans

- Business Continuity Policy
- Corporate Business Continuity Plan
- Business continuity plans for individual service areas
- Business continuity risks identified in the Corporate Risk Register
- Risk Management Policy and Framework
- Emergency Response Plan.