# A Corporate Business Continuity Plan Blueprint for Local Authorities

### January 2025

**Contents**

[Tables and Figures 3](#_Toc187323583)

[About our Blueprint Series 4](#_Toc187323584)

[Glossary 5](#_Toc187323585)

[1. Introduction 6](#_Toc187323586)

[1.1. Who should use this Blueprint? 6](#_Toc187323587)

[1.2. How is the Blueprint organised? 6](#_Toc187323588)

[1.3. How should this Blueprint be used? 6](#_Toc187323589)

[2. BC: A Definition 8](#_Toc187323590)

[2.1. What is BC? 8](#_Toc187323591)

[2.2. Standards 8](#_Toc187323592)

[2.3. How does BC differ to ICTDR? 8](#_Toc187323593)

[2.4. What is ICTDR? 8](#_Toc187323594)

[2.5. What is BCM? 10](#_Toc187323595)

[2.6. What are BCPs? 10](#_Toc187323596)

[3. BCPs: Developing, Mobilising and Reporting 11](#_Toc187323597)

[3.1. BCP considerations 11](#_Toc187323598)

[3.2. Establishing a BCMS 11](#_Toc187323599)

[3.3. Steps to consider 12](#_Toc187323600)

[3.4. Business impact analysis 13](#_Toc187323601)

[4. BCP: Stakeholders 14](#_Toc187323602)

[4.1. Who to involve? 14](#_Toc187323603)

[4.2. Individual examples 14](#_Toc187323604)

[4.3. Departmental resilience representatives 15](#_Toc187323605)

[4.4. Continuous improvement and staff capabilities 15](#_Toc187323606)

[Appendix 1: Corporate BCP Template 17](#_Toc187323607)

# Tables and Figures

[Table 1: Key stakeholders 13](#_Toc187237205)

[Table 2: Resilience representatives 13](#_Toc187237206)

[Figure 1: How to use this Blueprint? 6](#_Toc186551529)

[Figure 2: Interactions between BC and ICTDR 8](#_Toc186551530)

[Figure 3: BCMS governance 11](#_Toc186551531)

[Figure 4: BCP steps 12](#_Toc186551532)

# About our Blueprint Series

The Local Government Association (LGA) has developed a series of blueprints to support councils in England with cyber defence and resilience. They bring together a set of essential points to consider in managing, detecting, defending against and minimising the impact of cyber incidents. Each blueprint has been produced in line with the National Cyber Security Centre’s (NCSC) [Cyber Assessment Framework](https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework).

With the cyber threat landscape rapidly evolving, it is more important than ever that councils have robust strategies and plans in place to detect and respond to cyber-attacks. Our blueprints are intended to help councils with managing, and protecting against, cyber threats. We encourage councils to embed cyber resilience planning at strategic and operational levels to ensure the continuous delivery of critical services if and when a cyber incident occurs.

**Overview of Blueprint series**

No two councils are the same: each face different challenges within their respective environments. Our Blueprints, listed below, provide general guidelines for building strong cyber strategies to improve resilience that can be tailored to local contexts.

* [Cyber security and resilience blueprint series | Local Government Association](https://www.local.gov.uk/our-support/cyber-digital-and-technology/cyber-security-and-resilience-blueprint-series#:~:text=This%20blueprint%20has%20been%20developed,(NCSC)%20Cyber%20Assessment%20Framework.)

We recommend reading our Blueprints in conjunction with each other. If you would like to arrange a conversation with the LGA team about cyber resilience, please email cyberanddigital@local.gov.uk

**Disclaimer**

This Corporate Business Continuity Planning Blueprint for Local Authorities provides general guidelines and should be used as a reference. It is not a legal document and may not take into account all relevant local and national considerations. The LGA assumes no legal liability that may arise from the use of this document.

# Glossary

BC Business Continuity

BCI [Business Continuity Institute](https://www.thebci.org/)

BCP Business Continuity Plan

BCM Business Continuity Management

BCMS Business Continuity Management System

BIA Business Impact Analysis

CAF [Cyber Assessment Framework](https://www.ncsc.gov.uk/collection/cyber-assessment-framework)

CEO Chief Executive Officer

CISO Chief Information Security Officer

CTO Chief Technology Officer

DPO Data Protection Officer

DR Disaster Recovery

HR Human Resources

ICT Information and Communications Technology

ICTDR ICT Disaster Recovery

IR Incident Response

ISO [International Organization for Standardization](https://www.iso.org/home.html)

LGA [Local Government Association](http://www.local.gov.uk)

NCSC [National Cyber Security Centre](http://www.ncsc.gov.uk)

PR Public Relations

RPO Recovery Point Objective

RTO Recovery Time Objective

# 1. Introduction

## 1.1. Who should use this Blueprint?

This Blueprint is aimed at Strategic (Gold) and Tactical (Silver) levels of command in councils in England. We have developed this guidance to support corporate BC planning and to provide IR guidance. We suggest using this Blueprint when:

* Considering how to write or update a Plan.
* Starting conversations with colleagues involved in implementing the Plan.
* Collecting the information needed to support the development of an effective Plan.

BC planning at the Operational (Bronze) level via service leads is not the primary focus for this guidance, but relevant considerations are included.

## 1.2. How is the Blueprint organised?

This guidance has four sections:

* BC: A Definition
* BCPs: Developing, Mobilising and Reporting
* BCP: Stakeholders
* A Corporate BCP Template (to be completed based on a council’s requirements, resources and risk profile)

## 1.3. How should this Blueprint be used?

There is no single method for developing a corporate BCP. This Blueprint is best used as a starting point for developing a comprehensive corporate BCP based on acknowledged good practice in the local government sector. This Blueprint offers advice, but this should not be taken as assurance of the end goals, or the means in achieving them.

Figure 1 provides a suggested approach to using this Blueprint – to facilitate a joined-up approach to any existing service area approaches you may have.

**Figure 1: How to use this Blueprint?**

1. **Review the Blueprint:** Familiarise yourself with information in this Blueprint. Understand the overall structure and the purpose of each section. Note that business continuity is an ongoing effort, and the corporate BCP should be treated as a living document. Regularly revisit and update the document to ensure it remains relevant and effective.
2. **Gather organisation-specific information:** Identify the specific details and information unique to your council. This may include existing roles and responsibilities related to business continuity, governance structures, existing policies and procedures, risk assessment and business impact analysis results, regulatory requirements, and any other relevant information.
3. **Customise this Blueprint:** Replace the **templated text** in Appendix 1 with information specific to your council. Address the questions and consider relevant details and procedures aligned to your council’s needs and resources.

# 2. BC: A Definition

## 2.1. What is BC?

ISO 22301 defines business continuity as “an organisation’s capability to continue delivering products and services within acceptable timeframes, at predefined capacity, during a disruption”.

The BCI define it as “the strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level”.

## 2.2. Standards

BC standards are available, including non-statutory guidance accompanying the Civil Contingencies Act 2004, International Standards (ISO), and those promoted by organisations such as the Business Continuity Institute (BCI). Formal training, as well as experience, is likely to be of benefit to an organisation.

## 2.3. How does BC differ to ICTDR?

BC and ICTDR are two separate workstreams, but in recent times, their intersection has blurred due to widescale technology adoption. As outlined in our ‘ICT Disaster Recovery Planning Blueprint’, the ICT department is responsible for creating a service level BCP to ensure its critical activities (such as providing a customer service desk and ticketing system to the organisation) can continue to operate at predefined service levels. Additionally, ICT should work with areas of the business as they develop their resilience and continuity requirements to create DR plans setting out how they will respond to system interruptions affecting the entire organisation and applications used by individual services. For absolute clarity, ICT is a valuable contributor to overall BC planning – however, it does not lead the organisation on Business Continuity Management.

## 2.4. What is ICTDR?

We use a wide definition for ICTDR,which encompasses how ICT should plan for the continuity of its own services, and also contribute to the development of wider BCPs when technology is involved. You may feel this is differs to how the term is used in your organisation, where it may represent a single, technical solution to an event of system failure (e.g. “We’re switching System A over to DR, as the primary server has failed”.) These technical DR solutions are a valuable component in your resilience armoury, both for ICT in maintaining services, and for the organisation in terms of resilience and recovery. However, they are only part of the picture, and solely concentrating on them can detract from the fact that continuity is not just the responsibility of ICT. Figure 2 outlines some of the interactions between BC and ICTDR.

**Figure 2: Interactions between BC and ICTDR**



## 2.5. What is BCM?

Business Continuity Management (BCM) is a matter for a whole organisation. Leadership should ensure that their organisation has the right structure, roles, culture and processes to build resilience and responsiveness to multiple adverse events. It must also fund the agreed processes and their assurance.

As part of this, leadership should ensure that their organisation has proactively considered the potential risks and impacts that could disrupt operations. This is typically done through Business Impact Analysis (BIA) within a council’s operating areas. BIAs help an organisation understand the extent of disruption across its operating areas, helping to identify local priorities for restoration of services, functions and processes.

This list of priorities can offer a challenge to an organisation. Multiple areas will identify ‘priority one’ operations that need swift restoration. However, if resources are limited and choices must be made, then executives must determine which ‘priority one’ tasks are tackled first. This necessitates consolidating the findings of various BIAs and making corporate decisions.

## 2.6. What are BCPs?

Business Continuity Plans (BCPs) are drawn up to establish what an organisation will do to maintain its operations to an adequate pre-determined level, with an eye to their ultimate restoration. They set out necessary information, procedures and options so the organisation can be ready to respond when required. Cumulatively, all these structures and artefacts should enable ‘commanders’ and management teams to operate in an informed, structured manner during an event, taking necessary actions locally in their areas of responsibility, while handling pressing matters of prioritisation and working to counteract the unexpected and therefore unplanned for (‘crisis management’).

# 3. BCPs: Developing, Mobilising and Reporting

## 3.1. BCP considerations

BC continuity planning is a statutory requirement in England for all county, unitary and district councils and London boroughs including the City of London. However, maintaining statutory paperwork does not guarantee greater organisational resilience. There are many wider factors to consider, outlined in this section.

## 3.2. Establishing a BCMS

BCPs are one aspect of a larger system. A BC policy should outline the organisation’s high-level approach to BC governance and programme scope, and a framework document should describe the operational considerations for maintaining an effective BCMS. See **Figure 3**.

Considering all organisations are different in size, have different responsibilities, and have a unique risk profile, the scope of the BCMS should be proportionate to these factors and signed off at a senior level through the development of a BC policy. As an example, in addition to an overarching corporate BCP, county councils and unitary authorities might require a BCP for all services, whereas district authorities may choose to develop BCPs for the most critical services.

The scope of the corporate BCP needs to be considerate of, and potentially influence, other IR plans and frameworks across the organisation to avoid duplication. For example, Emergency Management Plans and existing ICTDR plans.

**Figure 3: BCMS governance**



## 3.3. Steps to consider

We outline in Figure 4, below, six steps to consider when developing a BCP, including working with stakeholders, seeking expert advice, reviewing and refining, obtaining approvals, communication and implementation, and a plan for monitoring, evaluating and updating.

**Figure 4: BCP steps**

* **Engage stakeholders:** Engaging stakeholders from the outset is an important first step to secure buy-in and to ensure that representatives from different functional services have an opportunity to feed into the process. It can also establish the council’s baseline systems, assets, risk management approach and security policies and processes. The specific individuals to be involved will depend on the size and structure of the council.
* **Seek expert advice if needed:** If you don’t have in-house expertise in business continuity, consider engaging external consultants or experts to provide guidance and assistance in developing plans. They can help ensure that BCPs align with industry best practices and address any specific challenges or requirements.
* **Develop, review and refine:** Once the initial draft is completed, review the entire corporate BCP document to ensure coherence, consistency, and completeness. Seek feedback from relevant stakeholders and make necessary adjustments.
* **Obtain approval:** Present the finalised corporate BCP to appropriate personnel and management groups within the council for review and approval. This may involve obtaining approvals from senior management, elected members, the ICT department, legal department, and other relevant decision-makers.
* **Communicate and implement:** Once the BCP is approved, develop a plan for communicating the BCP to all relevant employees and stakeholders. Ensure that everyone understands their roles and responsibilities and the next steps.
* **Monitor, evaluate, and update:** Continuously monitor the effectiveness of the plan, assess emerging risks, and evaluate the organisation’s cyber security posture. Regularly review and update the plan to address new threats, technologies, and regulatory requirements.

## 3.4. Business impact analysis

Gaining an understanding of the activities critical to an organisation, and the minimum viable service for these activities, can be achieved by conducting a BIA. The BIA will identify and rank critical services that need comprehensive BCPs and may need to be further prioritised by senior decision makers during a real-life incident response. The output of the BIA (critical activity information) is a primary feature of the corporate BCP. The BIA project should precede the development of BCPs to ensure a quantitative approach to BC planning, where ambiguity, errors and biases are minimised.

# 4. BCP: Stakeholders

## 4.1. Who to involve?

Developing a corporate BCP within a council requires the involvement of various stakeholders from different departments and in different roles. By involving all stakeholders, councils can foster a multi-disciplinary approach, ensuring that the BCMS reflects the organisation’s unique requirements and addresses potential vulnerabilities effectively. Collaboration among various departments promotes a shared responsibility and a holistic understanding of risks and associated mitigation strategies.

## 4.2. Individual examples

The specific individuals involved may vary depending on the size and structure of the council. Listed alphabetically, Table 1 provides examples of key stakeholders who might typically be included within the BCMS system governance structure to provide oversight, including during the development of a corporate BCP.

**Table 1: Key stakeholders**

|  |
| --- |
| * Audit officer: An audit officer can independently review and test security controls, mitigations and risk management processes that are in place.
* Business Continuity team: The primary team with day-to-day responsibilities ensuring the effectiveness of the business continuity management system. This may be joined with the Emergency Planning team in some organisations.
* Chief Information Security Officer (CISO): An ISO or equivalent role within the local authority is responsible for overseeing and managing information security.
* Data Protection Officer: A DPO or equivalent is responsible for overseeing and monitoring the council’s compliance with data protection legislation.
* Elected Members: Business continuity policies and procedures and their governance are owned by a cabinet portfolio holder.
* Emergency Planning team: Working on behalf of the organisation and with multiagency partners through the Local Resilience Forum to develop emergency plans.
* Executive Leadership: The senior management team, including the chief executive officer (CEO), chief information officer (CIO), chief technology officer (CTO), and Senior Information Risk Owner (SIRO), should be actively involved in the governance of business continuity.
* Information Governance Officer: An IGO or equivalent role will be responsible for overseeing data protection compliance.
 |

## 4.3. **Departmental resilience representatives**

Including representatives from different departments within the BC governance structure is crucial to understanding the specific needs and challenges faced by each department, in addition to supporting the flow of information during an incident response. Representatives from finance, legal, planning, social care, revenue and benefits, housing and other relevant departments can provide valuable insights and requirements, in addition to creating their own service level BCPs to supplement the corporate BCP. See Table 2.

**Table 2: Resilience representatives**

|  |
| --- |
| * Communications and Public Relations: As incidents can impact public trust and reputation, involving communications and PR professionals is essential. They can assist in creating effective communication plans, managing public relations during incidents, and ensuring consistent messaging to stakeholders.
* Human Resources/Learning and Development: HR personnel can contribute by addressing the human element of BC.
* ICT Department: The ICT department plays a critical role in the protection of digital infrastructure by implementing cyber security and disaster recovery measures. ICT managers, network administrators, system administrators, and other ICT staff members possess valuable technical knowledge and insights that need to contribute to the corporate BCPs development and any service area plans.
* Legal and Compliance Team: Involving legal and compliance professionals ensures that BCPs align with legal requirements and regulations.
 |

## 4.4. Continuous improvement and staff capabilities

To minimise the disruption caused by an incident, IR exercises should be conducted at all levels of command (Strategic (Gold), Tactical (Silver), Operational (Bronze)) to familiarise staff with their defined roles and responsibilities and to rehearse and embed key procedures (such as activating command structures). Audits, annual plan reviews, and annual exercises, validate corporate and service level BCPs.

|  |
| --- |
| **All information below should be used as a guide. Guidance text should be replaced with your council’s information before publishing a final copy. Any remaining guidance text should be deleted.**  |

# Appendix 1: Corporate BCP Template

[Local Authority Name]

**OFFICIAL – SENSITIVE**

**Version:** [Enter version reference]

**Issued Date:** [Enter date]

**Review Date:** [Issue date + 1 year]

**Signed-off by:** [Strategic owner]

This document must be kept secure and up to date as it contains personal information.

**Amendment Record**

|  |  |  |
| --- | --- | --- |
| Issue No | Date | Detail of amendment and name |
|  |  | [Enter details about document updates] |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Exercise Record**

|  |  |  |
| --- | --- | --- |
| Issue No | Date | Detail of exercise and participants |
|  |  | [Enter details about corporate exercises] |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Distribution list**

|  |  |  |
| --- | --- | --- |
| Copy No | Issued to | Title |
| 1 | [Enter name] | [Enter role] |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |
| 6 |  |  |
| 7 |  |  |
| 8 |  |  |
| 9 |  |  |
| 10 |  |  |
| 11 |  |  |
| 12 |  |  |
| 13 |  |  |
| 14 |  |  |
| 15 |  |  |
| 16 |  |  |
| 17 |  |  |
| 18 |  |  |
| 19 |  |  |
| 20 |  |  |
| 21 |  |  |
| 22 |  |  |
| 23 |  |  |
| 24 |  |  |
| 25 |  |  |
| Physical Copy stored at: [Enter location]Electronic Copies stored at: [Enter location] |
| Copy stored in Grab bag at: [Enter location] |
| In addition to the list above, individuals may be given access to this document if they are given a role during the response to an incident. |

**Foreword**

|  |
| --- |
| [The corporate business continuity plan (BCP) should be introduced by the relevant portfolio holder or member of the Executive Leadership team within a council, outlining ownership and/or political buy in. They should champion the commitments set out in the business continuity policy, providing a link to the relevant document. The foreword should provide an overview of the vision and aim behind the corporate BCP, why it is important, how it fits in with wider council documents, and its benefits in protecting local communities through the protection of key council assets. It should summarise the local authority’s commitment to business continuity and safeguarding against cyber threats. You should describe how this relates to and empowers other areas of work, e.g., the council’s digitalisation strategy, ICT strategy, and council-wide plan.]EXAMPLE: Should [Council] suffer an incident that could potentially disrupt service delivery it is important to ensure services can continue to function at an acceptable level. [Council] must ensure it has 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 (CCA) 2004.The Corporate Business Continuity Plan is the overarching BCP for [Council]. Departments have their own BC plans, and all teams should have operational BC plans in place; these contain comprehensive information to ensure that individual services and teams can continue to operate regardless of any incident.It is the responsibility of all of us to ensure our BC plans and arrangements are created, communicated, validated and updated regularly so we can collectively ensure we are able to deal with any incident that may come our way. |

**Introduction**

|  |
| --- |
| [The corporate BCP should be introduced by building on the foreword and providing more detail about the requirement for effective BCPs and key considerations, projects and partners supplementing the contents of the corporate BCP.]EXAMPLE: This plan sets out the overarching response mechanisms for business continuity incidents. Under the Civil Contingencies Act 2004, [Council] is classed as a Category 1 responder, with a statutory responsibility to be able to respond to and recover from major incidents. The scale of [Council], and the diverse nature of services delivered, means that we need to have robust arrangements in place to be able to respond to incidents that may affect us. Ensuring that we have our internal Business Continuity arrangements in place, will help ensure that our wider responsibilities as part of the Local Resilience Forum are met effectively and efficiently. Other documents related to this plan:[Link to relevant documents] |

**Purpose**

|  |
| --- |
| EXAMPLE: The purpose of this plan is to enable the organisation to continue to deliver its critical functions at an acceptable predefined level in the event of an incident. This plan will set out the following:* Incident management arrangements for a major incident.
* Detail activation and escalation procedures.
* Detail the roles and responsibilities of key personnel during a major incident.
* The agreed list of critical activities which are essential to the authority.
* Non-critical activities which could potentially be suspended for a period of time.
* Supporting documents to assist in incident management e.g., meeting agendas/checklists and so on.

This plan does not provide detailed information on particular departments or service level business continuity arrangements – this information can be found through departmental and service level plans. |

**Section 1: Incident Management**

[This section should document the coordination structures that will be activated to manage an incident and define the parameters and criteria for the extent of internal escalation. For example, how disruptive or long lasting does a major incident need to be? Be specific. What are the trigger points? Would any incident with a potential for reputational damage be a major incident?]

Incidents affecting [Council] services will normally fall into one of the following three categories:



**1.1 Major Incident:**

EXAMPLE:

* A major incident will require activation of the Strategic (and Tactical) coordination group.
* The corporate BCP will be activated, in addition to the service level BCPs for affected teams.

**1.2 Moderate Incident:**

EXAMPLE:

* A moderate incident will require activation of the Tactical coordination group, with updates to Strategic as required.
* Departmental and service level BCPs will be activated for affected teams.

**1.3 Minor Incident:**

EXAMPLE:

* Business as usual with impacts managed solely by the affected service within incident management teams (IMTs).
* No requirement to activate Tactical or Strategic coordination groups.
* For a major incident all levels of command will be established. For moderate incidents, the Tactical group will usually be formed, this group will report into the Strategic group (if established). The Strategic group may not meet formally but will need to be kept updated.
* IMTs will be conducted at the operational level to manage impacts to service, and the Tactical representative will feed IMT issues into the Tactical discussion.
* Depending upon the incident a full Tactical group may meet, or alternatively individuals representing specific departments or specialist areas will be invited.

**Section 2: Roles and Responsibilities**

[This section should document the overarching roles and responsibilities of the above coordination groups, and then define the membership of, and individual roles and key interactions within these groups. The development of RACI (Responsible Accountable, Consulted, Informed) matrices can outline the roles and responsibilities for each activity within a larger process, which can be added into the appendices as a quick reference guide for incident responders.]

**2.1 Strategic (Gold) Response Group**

EXAMPLE: The Strategic group should be called together in any incident which could have (or is having) a major impact on service delivery. It will comprise of the senior leadership team and the Head of Resilience. The nature of the incident will determine which other functions will need to be in attendance. The Head of Resilience will advise on additional members that may need to attend the Strategic group. Its meeting location will be confirmed at the time and may be via Microsoft Teams call. The decision to call the Strategic group together will be taken by the Chief Executive or nominated representative (Duty Director for example).

**Membership**

EXAMPLE: The Strategic group may consist of the following members:

* Chief Executive or Duty Director (Chair)
* Senior leadership team members/deputies
* Relevant Heads of service - Head of Communications, Head of HR, Head of ICT
* Specialist representation for example Fire and Rescue Service/Public Health/Trading Standards/Highways
* Media/Public Relations
* Chief Legal Officer
* The Head of Resilience (staff officer to the Chief Executive/Duty Director)
* Partner/external organisations
* Emergency Support Staff (Loggists)

**Responsibilities**

EXAMPLE:

* To agree and provide the overall response and communications strategy.
* To assist the Tactical group by providing adequate resources for the response and recovery to the incident, including authorising expenditure.
* To provide visible leadership, and to motivate and encourage staff to participate in the management effort as required.
* To communicate incident information to Tactical group, staff, customers and other central and local government organisations as appropriate.
* Oversee the management of media and communications, including to Elected Members.

**2.2 Tactical (Silver) Group**

EXAMPLE: The Tactical group will coordinate the response to the incident and will report to the Strategic group. Depending upon the type of incident, the core Tactical group will be called together, with some extended membership, such as some resilience representatives, specialist staff and members of the Resilience team. The Tactical group will focus on the continuity of critical services. Individuals must ensure their department is represented if they are unable to attend a meeting themselves. The Tactical group’s meeting location will be confirmed at the time of the incident and is likely to be [via MS Teams, if operational].

**Membership**

EXAMPLE: The Tactical group may include the following members:

* Chair – Duty Director or nominated senior manager
* Head of Resilience
* Senior Resilience Officer
* Resilience Officer(s)
* Head of service(s) affected
* Communications Officer
* Health and Safety advisor
* Resilience representatives such as HR, Health and Safety, ICT, Estates, Finance, Fire and Rescue Service, Risk, Comms, staff representing area affected.
* Business Support/ Support staff loggist
* Other specialist staff required to maintain / restore services

Note: The liaison between the Strategic group (if formed) and the Tactical group is usually via the chair of Tactical.

**Responsibilities**

EXAMPLE:

* Overall coordination and management of the incident in line with the strategy set by the Strategic group (if formed).
* To brief the Strategic group, if formed.
* To cascade information to departmental managers.
* Keep a detailed log of the incident.
* To ensure all Heads of Services can communicate with their staff.
* To supply relevant information regarding any changes made to their department’s resource requirements.
* To provide a situation report when required.

**2.3 Operational Group (Incident Management Team - IMT)**

EXAMPLE: This will usually comprise staff from within the team or department affected and will be responsible for maintaining/recovering critical activities through IMT meetings. They take direction from the Tactical group and keep them updated. They will need to communicate any issues or concerns to the Tactical group to ensure that issues can be managed in a coordinated way.

**Membership**

EXAMPLE:

* Dictated by the service and documented in service level BCP.

**Responsibilities**

EXAMPLE:

* Ensure critical activities are maintained.
* To assist with the recovery of services.
* To relocate to alternative premises, if required.
* To liaise with the Tactical group for requests for assistance / resources if required.
* To provide updates when requested by the Tactical and Strategic groups

**2.4 Elected Members**

EXAMPLE: If Strategic/Tactical agree that help is needed from elected members, democratic services/communications will make contact asking for support. The role in an incident and in the recovery of an incident is listed below.

**Incident Response**

EXAMPLE:

* Supporting the response with local knowledge – particularly identifying vulnerable individuals/groups.
* Supporting and providing reassurance to their affected community with information received from corporate communications.
* Supporting the officers involved in the response.
* Acting as a community leader and channelling information to the public.
* Providing coordinated information to the media, avoiding mixed messages.
* Being aware of the latest situation by attending briefing sessions (if required)

**Incident Recovery**

EXAMPLE:

* Providing a political lead on the way in which decisions are made.
* Being a champion and supporter of the community.
* Using local knowledge and community contacts to identify priorities and resources.
* Assisting with VIP visits.
* Representing their community.
* Supporting efforts to repair and reconstruct the affected community if applicable.
* Promoting joint working
* Liaising with other elected representatives including MPs.
* Seeking additional resources and financial assistance from Government.
* Approving any regeneration issues.
* Involvement in the management of any appeal funds and memorials.

**Chief Executive / Strategic Chair**

EXAMPLE:

* Assume overall responsibility and Strategic coordination of all measures to deal with a major incident.
* Attend Strategic Coordination Group (if the situation is part of a wider emergency) or nominate an Executive Director.
* Ensure the Duty Director is able to coordinate and manage the Tactical response as required.
* Be responsible for authorising the commitment of resources and financial expenditure.
* Establish and chair Strategic group meetings.
* Determine media strategy in respect of the incident.
* Ensure stakeholders kept informed, particularly on policy and financial matters.

**Duty Director (or nominated Director)**

EXAMPLE:

* Coordinate and manage the Tactical response to the incident.
* Chair the Tactical group or nominate another person to lead the Tactical group.
* Be a member of the Strategic group and provide briefings as appropriate.

**Head of Resilience/Senior Resilience Officer**

EXAMPLE:

* Provide initial assessment of the incident.
* Advise the Chief Executive (Duty Director/chair) of developing incidents.
* Ensure appropriate expert advice is sought where necessary in a timely way.
* Staff Officer to the Chief Executive/Duty Director.
* Activate the Strategic Coordination Centre and advise relevant managers.
* Alert appropriate representatives to attend Tactical group meetings, when required.
* Ensure Tactical group and Resilience representatives are made aware and kept up-to-date on developing incidents.
* Ensure detailed records of actions taken during and after the incident, including expenditure are maintained.
* Ensure that the lessons identified from any incident are widely disseminated to everyone concerned and that Business Continuity plans are updated accordingly.

**2.8 Resilience Team**

EXAMPLE: Provide the groups (Strategic and Tactical) with support to enable them to manage the situation.

* Ensure the Communications team keep staff aware of developments and updates.
* Monitor effectiveness of communications between staff and teams.
* Organise help and assistance from other departments or groups if requested on a mutual aid basis.
* Ensure incidents are assessed in line with the incident escalation process, and that departments affected are aware and kept up to date.
* Ensure that existing documents and procedures are followed/used.

**2.9 Health and Safety**

EXAMPLE: Provide advice to staff, members and the public on threats to communities’ and/or individual’s health.

**2.10 Customer Service**

EXAMPLE:

* Ensure the website is updated at regular intervals.
* Ensure staff rotas are organised to manage an increased demand in calls if the incident requires this and a dedicated line is established if required.
* Liaise with other services to ensure a staff incident line is available if needed.

**2.11 Democratic Services**

EXAMPLE:

* Communicate with Elected Members on behalf of the Strategic group if requested by Communications.
* Deal with enquiries from Elected Members and organise briefing sessions if required.
* Ensure all Elected Members are briefed on the incident and its impact on services.

**2.12 ICT Services**

EXAMPLE:

* Liaise with relevant parties regarding ICT requirements, provide updates on progress of recovery if applicable.
* Organise the recovery of infrastructure and systems in line with critical activity requirements and business need.
* Identify and order replacement equipment as necessary.
* Escalate incidents and request a Tactical meeting is called where required.
* Brief the Resilience team on ICT related incidents, as soon as information is available and agree the cascade of this information to Resilience Representatives.
* Organise additional support to reinstate infrastructure and systems if necessary.
* Support services in providing system data required for Tactical meetings where required.
* Visit alternative sites (if applicable) to advise on ICT requirements.

**2.13 Human Resources**

EXAMPLE:

* To ensure processes are in place to deal with employment issues and advice at short notice.
* To employ an alternative system of recording if ICT is affected or absence data is required quickly.
* To provide management information to support the decision-making process.
* To advise on any matters relating to Employment Law.
* To support the continuity of services by examining the flexibility and deployment of the workforce and to discuss the potential for allocation of additional staff if necessary.
* To ensure the Tactical group are aware of, and work in line with, relevant HR policies and guidance.

**2.14 Insurance**

EXAMPLE:

* Liaise with the insurers, as appropriate.
* Advise Tactical and Strategic groups on insurance matters.
* Attend Tactical group meetings or ensure a nominated representative attends.

**2.15 Risk Management**

EXAMPLE:

* Provide advice and guidance on risk management.
* Input into the debriefing process including the analysis of risks following an incident.
* Monitor, review and challenge risk management activity.

**2.16 Facilities**

EXAMPLE:

* Brief Tactical group regarding the condition of any buildings affected.
* Liaise with the team seeking alternative accommodation to advise on suitability and technical matters to include security, car parking.
* Control or provide advice on the evacuation of premises.
* Brief security personnel, if necessary, to patrol the affected parts of the building after discussions with the insurers.
* Provide staff to assist with the relocation of services.
* Provide catering facilities to staff where required.
* Provide cleaning facilities and staff where appropriate.
* Provide security personnel where appropriate.
* Provide equipment/resources where possible to assist the recovery process.
* Provide transport for moving staff to alternative locations where necessary.

**2.17 Estates Team**

EXAMPLE:

* Alert/liaise with Facilities and Resilience team regarding any incident that has the potential to disrupt services.
* Provide information on alternative buildings where necessary.
* Identify and assess alternative accommodation where necessary.
* Organise technical experts in the event of a crisis affecting part of a building and to report progress back to Tactical group at frequent intervals.
* Provide contractors where necessary for emergency building.
* Provide guidance on evacuation, bomb threats, suspect/actual attacks.

**Business Support**

EXAMPLE:

* Provide administrative support/ meeting loggist function for all Strategic and Tactical meetings.
* Provision of support staff.

**2.19 All other teams/service areas**

EXAMPLE:

* Ensure Resilience Representatives attend Tactical meetings as needed.
* Provide information as required to Tactical for inclusion in situational reports.

**Section 3: Communications**

[This section should outline the initial activation of the communications team and process relevant to their contribution to an incident response, such as effective information management to internal and external stakeholders, ensuring consistent communications to all stakeholders.

The activation and management of a dedicated communications cell to support the Tactical group should also be considered in this section. This will provide guidance for the communications cell liaison with multiagency partner communications teams, i.e., Police or other local authority communications team to ensure consistency of messaging.

Furthermore, PACE (Primary, Alternative, Contingency, Emergency) communications should be a consideration of this section to outline which communications platforms will be used under certain conditions. For example, how would you communicate with internal staff if primary communications platforms such as Microsoft Teams and Outlook where unavailable? What are your Alternative arrangements?

Further information about crisis communications can be found in this LGA resource:

[Crisis communications – cyber attack | Local Government Association](https://www.local.gov.uk/our-support/guidance-and-resources/comms-hub-communications-support/cyber-attack-crisis)]

EXAMPLE: The first point of contact during office hours would be any member of the Communications team and, after hours, the on-call duty Communications Officer.

A Senior Communications Officer will sit on Strategic and/or Tactical groups. These officers would liaise directly with the Communications team. This would enable correct, agreed messages to go out to both the media/public and our own staff/partners.

The Communications team must ensure that all relevant services are consulted with before acting. In some instances, specialised advice will be required.

Messages will be communicated through various methods including:

* Social media in line with social media guidelines
* Internet/Intranet
* Email

Communications will engage with the media and deal with all press enquiries as appropriate and they will produce regular agreed press statements from the Tactical, or Strategic group if formed.

For further information and pre-scripted messages, please see the Communication’s team emergency plan.

**PACE (Primary, Alternative, Contingency, Emergency) Communications**

EXAMPLE: (You should also consider where face-to-face communication may be required):

|  |  |  |  |
| --- | --- | --- | --- |
| Method | Platform | Platform Owner/contact | Activation/Further Information |
| Primary | MS Teams | Name:Contact: |  |
| Email | Name:Contact: |  |
| Alternative | Corporate mobile phones | Name:Contact: |  |
| Intranet | Name:Contact: |  |
| Contingency | WhatsApp | Name:Contact: |  |
| Personal devices | Name:Contact: |  |
| Emergency | Airwave radio  | Name:Contact: |  |
| Printed messages | Name:Contact: |  |

**Teleconference Protocols**

EXAMPLE:

This is how a teleconference will be called to manage an incident:

**Multiagency Major Incident Communications Cell**

Should the incident result in a multi-agency Strategic/Tactical Coordinating Group (SCG/TCG) meeting (s) being convened:

* A multi-agency Communications Cell would be established to coordinate communications around the incident. Communications will send a representative there.
* The Strategic Communications Lead would attend the Strategic Coordination Group to agree key messages and ensure information and decisions are shared with the Media Cell.

The Strategic Communications Lead (SCL) has responsibility over the content of external communications about the incident. If the incident is one which requires activation of this plan, internal communications will still need to be managed from within [Council], in consultation with the SCL as appropriate.

**Section 4: Critical Activities**

[This section contains the output of a Business Impact Analysis (BIA) and summarises departmental level business continuity plans by displaying the most critical activities only\* - those that the organisation must continue to operate, even during a significant incident like a ransomware attack. The purpose of this information is to provide decision makers with guidance as they define the strategy and re-allocate resources to manage an incident response.

\*These activities would cause a “major” or “extreme” impact within 1 week if they could not be delivered - resulting in significant negative coverage in national media, significant impact to service users and/or non-delivery of council objectives.

The BIA should define the impact rating criteria underpinning the analysis to provide tangible metrics to terms such as extreme, major, moderate, minor and insignificant. These impact ratings should be considered across a range of themes, including service delivery, health and safety, financial loss, performance, reputation, environment and so on. This will support services to create their impact assessment, accurately reflecting how critical their service is, rather than estimating. The impact assessment is directly linked to the Recovery Time Objective (RTO) for that service. For example, a service with activities that have an ‘extreme’ impact rating (i.e., significant financial loss in day one of an incident) will be an ‘immediate’ recovery priority. This will be a critical activity, and therefore a critical service.

When considering Recovery Point Objectives, services will need to discuss service level agreements with ICT suppliers and understand the unique setup of their service infrastructure.]

When figuring out how much data a service can afford to lose in a disaster (Recovery Point Objective), it's crucial to have a chat with your IT suppliers. This conversation should cover the specifics of your service level agreement (SLA) and get a good grasp of how your service's infrastructure is set up. This understanding is key because:

SLAs outline expectations: Your SLA with the supplier will detail what they're responsible for in a recovery scenario, including how quickly they need to get things back up and running.

Infrastructure impacts recovery options: The way your service is built will determine what recovery options are available and how effective they'll be. For example, if your data is spread across multiple locations, you'll have more flexibility than if it's all in one place.

By having this discussion, you can ensure that your Recovery Point Objective is realistic and aligns with what your supplier can actually deliver. This will help you avoid nasty surprises and ensure your business can bounce back quickly from any unexpected events.

EXAMPLE:

**Department 1**

|  |  |  |
| --- | --- | --- |
| Adult Social Services Department | 24/7 Service | Impact assessment |
| Example: Conduct mental health assessments  | Y | Immediate |
| Example: Safeguarding | Y | Immediate |
| Example: Pay careers | N | 1 day |
|  |  |  |
|  |  |  |

**Department 2**

|  |  |  |
| --- | --- | --- |
| Cross departmental | 24/7 Service | Impact assessment |
| Example | Y | Immediate |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Department 3**

|  |  |  |
| --- | --- | --- |
| Cross departmental | 24/7 Service | Impact assessment |
| Example | Y | Immediate |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Section 5: Post Incident Activity**

[This section should provide guidance to decision makers on activity that will follow the incident response and recovery, ensuring that staff are debriefed and lessons are captured in a post incident report for continuous improvement. Relevant blueprints for the post incident report should be created and linked within this document.]

EXAMPLE: Following any major or moderate incident, steps will be taken to capture lessons identified that can enhance resilience in the future. All levels of incident management that were activated will be debriefed e.g. Strategic, Tactical, Operational.

The report should be independent and not created by anyone that was heavily involved in the response or recovery. The report is normally compiled by the Resilience team in collaboration with specialists from the affected services. The report will include an incident summary, details of feedback obtained from debriefing and recommendations/actions to take forward to implement lessons identified. All responses received on which the report is based should be included in the appendix.

The action log will be maintained and updated by the Resilience team.

In a cyber security incident, ICT will also complete a separate, but related, ICT report to ensure technical lessons are effectively managed.

**Section 6: RACI (Responsible, Accountable, Consulted, Informed) Matrices**

[This section is used to define the roles and responsibilities associated with various steps within a process. These processes might be generic, e.g. how to setup Strategic and Tactical Command, or they could be specific, e.g. how to respond to ransomware incident, a fire in a key building, or loss of a critical supplier to the authority.]

EXAMPLE:

**Cyber Security Incident**

A Cyber security incident has the potential to cause total loss of ICT or a degradation of service. Any incident over 24 hours duration would be considered a “Major Incident”. ICT Services will take preventative controls to mitigate any incident. ICT Services would contact the Resilience Team to initiate Tactical and Strategic coordination if necessary.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Action | ICT Infrastructure Manager | Head of ICT | Resilience Team | Comms |
| 1. Identification of cyber attack | R | A | C | I |
| 2. Declaration of cyber security incident | C | A | R | I |
| 3. Internal messaging to staff | C | C | C | R, A |
| … |  |  |  |  |

**Section 7: Responder Checklists**

[This section is used to outline roles and responsibilities associated with individual responders at the Strategic and Tactical levels. These might be generic considerations which are relevant to wide range of incident (e.g. maintain a decision log), or they could be specific, e.g. the Director of ICT activating the disaster recovery plan.]

EXAMPLE:

**Director of ICT**

The following actions are those that the Director of ICT should consider.

|  |  |
| --- | --- |
| Consideration / Task | Completed |
| Nominate a Deputy to assume responsibilities during absence. |  |
| Open a personal decision log within the area of responsibility.  |  |
| Establish departmental meetings to brief managers.  |  |
| Ensure critical ICT infrastructure continues to operate/may be brought into operation during an incident, assess additional risks/dependencies that may exist. |  |
| Activate Business Continuity plans if required. Activate Disaster Recovery plans if required. |  |
| Ascertain multi-agency groups that ICT need to link to, and any that ICT need to chair. Ensure links to other agencies are established. |  |
| Be prepared to represent the council at TCG and attend StrategicIdentify staff to represent at Tactical. |  |
| Consider support that may be requested from other organisations – can support be provided if requested? |  |
| Advise Heads of Service or other appropriate personnel on matters affecting ICT systems, which may have occurred because of the incident response. |  |

**Section 8: Standard Agenda**

[This section is a standard incident response agenda. It may be necessary to produce different agendas for Strategic and Tactical response groups. It is important to keep an agenda in the plan to centralise all information for activating an incident response. You should assume you have lost the corporate network where all other documents and blueprints are saved. At least you have a printed corporate business continuity plan in a grab bag with the key information.]

EXAMPLE:

* Attendees – (and confirmation of required attendees)
* Apologies
* Matters arising requiring urgent decisions / actions
* Approval of previous notes/actions
* Actions from previous meeting(s) – Action Log
* Situation Report (including update from Tactical group )
* Update from all departments (including impact on critical activities)
* External updates (if applicable)
* Establishment / Review of strategy
* Communications Strategy, Internal / Elected Members / External
* Any other urgent business
* Summary of actions allocated during this meeting
* Date / time of next meeting

All key decisions should be recorded in the notes and actions recorded on the action log.

Ensure meeting minutes and action log are circulated to the Tactical group and Strategic groups.

**Section 9: Action Log Blueprint**

[The action log is a management tool which is required to formally track incident response activity and to ensure actions are completed by their owners. It is also critical to capture decisions that are taken in coordination meetings, and a decision log blueprint can be designed and implemented in parallel to the action log.]

EXAMPLE:

|  |  |
| --- | --- |
| Incident:  | Meeting date (s) |
| Last Updated: | Meeting times: |
| Loggist:  |
|  | Action / Issues | Owner | Update | Status |
| 001 |  |  |  |  |
| 002 |  |  |  |  |
| 003 |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Section 10: Combined Situation Report**

[Situation reports are a key method of information management during an incident response - passing information from the operational responders in IMT, to the strategic decision makers in their group. It is important to maintain a shared situational awareness across the organisation so decision makers can base their decisions on accurate information.

It may be necessary to have several versions of the Situation Report blueprint. For example, a service level situation report blueprint which IMT’s use to define service level impact and escalate issues to Tactical. This is supplemented by the combined situation report blueprint which Tactical use to collate all service level responses, review/analyse, and then prioritise these escalations to involve Strategic as required.]

EXAMPLE:

|  |  |
| --- | --- |
| Incident:Time:Date: | Ransomware0900Wednesday 1 January, 2025 |
| Background Information:  | Following ransomware deployment on the corporate network on Sunday, there is wide scale disruption across the organisation and all departmental business continuity plans have been activated and are using documented workarounds to continue critical activities. Strategic and Tactical are also both activated.  |
| Key Issues/escalations:  | Access to e-mail and teams currently interrupted. Escalated to STRATEGIC for consideration of options. |
| Current Situation of Departments |
| A) Department |
| Team 1 |  |
| Team 2 |  |
| B) Department |
| Team 1 |  |
| Team 2 |  |
| … |  |

**Section 11: Contact Details**

**Strategic Group**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Role | Work no | Home no | Mobile no |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Tactical Group**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Role | Work no | Home no | Mobile no |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Directors**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Role | Work no | Home no | Mobile no |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Department Leads**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Role | Work no | Home no | Mobile no |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Support Staff**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Role | Work no | Home no | Mobile no |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**24/7 On-call**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Role | Phone number  | Email |
|  | Resilience |  |  |
|  | Communications |  |  |
|  | Highways |  |  |
|  | Social Care |  |  |