Corporate Business Continuity Plan for

Comhairle nan Eilean Siar

Version number	4 draft
Plan owner	Chief Executive
Depute owner	Head of Law and Governance
Plan developed by	Finance & Risk Management Officer
Last approved	19-June-2024
Last test date	21-November-2023

Table of Contents

1.0 Introduction

Comhairle nan Eilean Siar provides public services across the Outer Hebrides. This plan sets out how the Comhairle will continue to deliver its critical services in times of disruption. The priority list for the critical services is a live document which is updated as services revise and test Service Business Continuity Plans (BCPs). Corporate Management Team and Elected Members have access to this Business Continuity Management SharePoint page.

This is an overarching plan for senior management to refer to in the event of a major incident. Service Business Continuity Plans contain the details for the specific services.

The **Continuity Plan** is intended to be the main reference document. It sets out the generic response to any **Incident**. **Service Recovery Teams** may have decided to create **Specific Response Plans** to address specific scenarios defined during the Risk Assessment step (see Appendix A for an example of a Specific Response Plan).

The Corporate Business Continuity Plan is integrated with Service BCPs and Disaster Recovery Plans (DRPs), and therefore assumes that all Service BCP's and DRP's are up to date, tested and reliable.

2.0 Distribution list / key people

Name	Role	Out of Hours contact	Depute	Depute Out of Hours contact
Chief Executive	Able to declare a Comhairle wide Incident		Chief Officer, Law and Governance	
Chief Financial Officer	Release funds		Principal Accountant	
Chief Officer, Law and Governance	Monitor the legal aspects of the Recovery		Solicitor (AM)	
Democratic Services Team	Clerk meetings Other administrative tasks		Democratic Services Team	
Chief Officer, Human Resources & Performance	HR lead Main contact for liaising with the Incident Team		Resilience & Training Manager	

3.0 References and related documents

Document Title	Location	Contact	Depute
Business Impact Analysis	Service BCPs / Business Continuity Management	Chief Officers	As named in Service BCP
Risk Assessment	Corporate Risk Assessment	Finance & Risk Management Officer	Resilience & Training Manager
Contact List – Staff	Service BCPs	Heads of Service	As named in Service BCP
Contact List - Internal stakeholders	Service BCPs	Heads of Service	As named in Service BCP
Contact List - External stakeholders	Service BCPs	Heads of Service	As named in Service BCP
Contact List – Suppliers	Service BCPs	Heads of Service	As named in Service BCP
Resilience Planning Team documents	Resilience Direct	Resilience & Training Manager	Corporate Management Team
Site Disaster Recovery Plan		Chief Officer, Property and Infrastructure	As named in DRP
IT Disaster Recovery Plan		IT Manager	As named in DRP

Service-specific documents and corresponding information can be found within the Service Business Plans.

4.0 Aims and objectives

4.1 Aims

Following a major incident impacting multiple services, this plan is intended to assist Comhairle nan Eilean Siar in recovering its critical services within the timescales assessed during Service's Business Impact Analyses.

4.2 Objectives

To detail the agreed response to a major business disruption and identify key contacts during an emergency, using critical services as identified in Service's Business Impact Analyses. The Risk Assessment carried out in relation to the Corporate Business Continuity Plan, ranks the risks most likely to cause a business interruption, allowing the prioritisation of risk reduction activities.

This information has been communicated to services for consideration in their plans.

5.0 Plan assumptions

For this Plan to work, the following assumptions have been made:

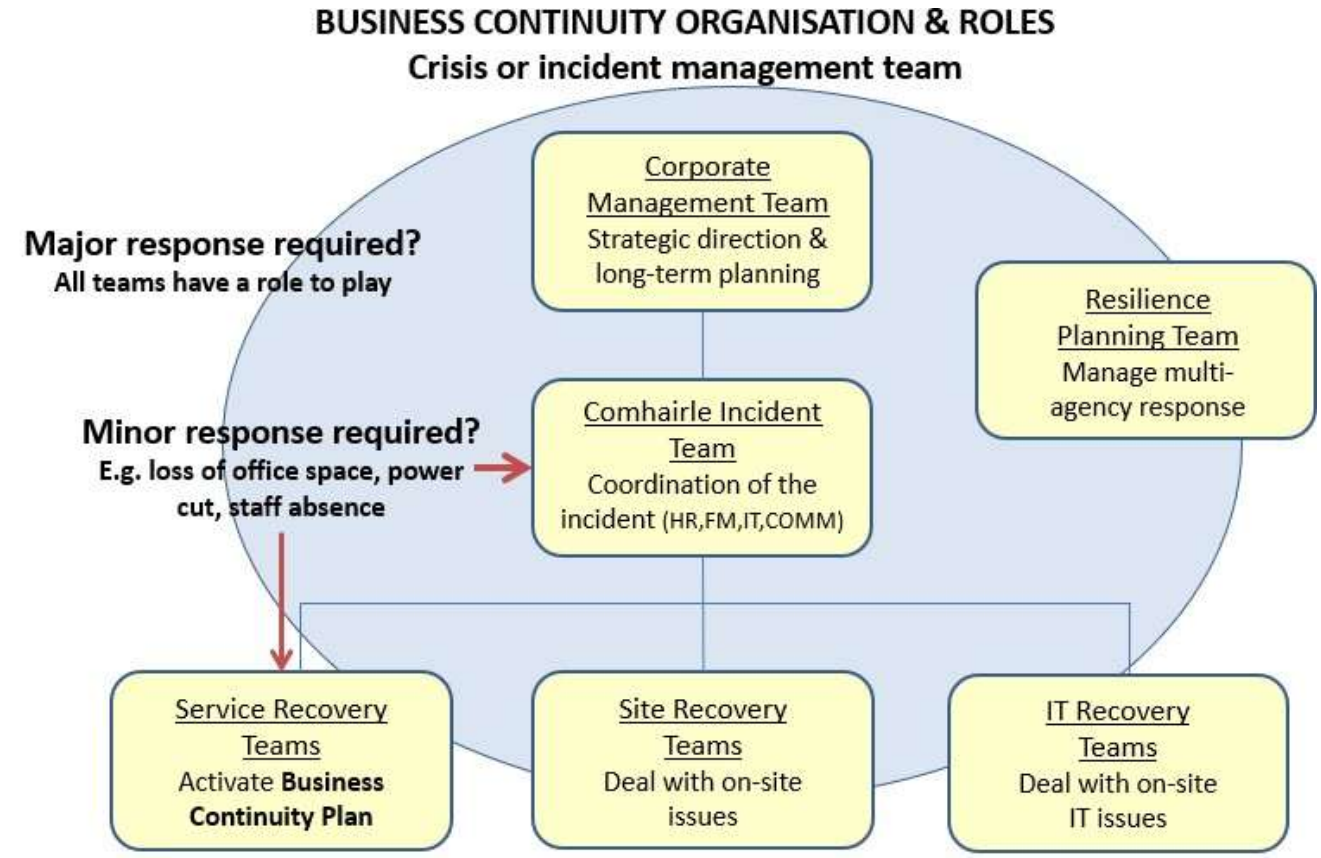
Disaster Recovery Plans are in place and up to date for work premises and Information Technology.

Service Business Plans referred to throughout the Corporate BC Plan are up to date and tested.

All lists mentioned in the Plan are up to date and available off-site, i.e. Staff Contact list, External Stakeholders.

6.0 Comhairle Nan Eilean Siar Incident Management Structure

The Incident Management Structure teams are shown on the following diagram. In the event of a major incident, all teams have a role to play. During a minor incident, the Comhairle Incident Team and the relevant Service Recovery Team should be notified to activate the Service BCP.



This is where BC Plans sit within the Incident Management Structure!

7.0 Comhairle Nan Eilean Siar Incident Management Structure – Responsibilities

Corporate Management Team (Strategic)

- To agree the strategic direction and long-term planning in relation to the major incident
- Release funds
- Determining corporate level communications strategy, including external and internal actions to be undertaken by the Comhairle Incident Team
- Monitor the legal aspects of the recovery

Comhairle Incident Team (Tactical)

- Comhairle wide management of crises, disruptions, and incidents
- Assess the situation by gathering information from as many sources as possible
- Agree an action plan to protect human life, the environment, organisational assets and the future viability of the service
- Always have an up-to-date Communications Strategy in place and communicate with key (internal and external) stakeholders throughout the incident
- Review progress throughout any disruption and take appropriate decisions to get back to normal operations
- Ensure lessons are learned following any crisis, disruption or incident
- Coordinate the Service Recovery Team
- Coordinate the recovery of a building, financial aspects and media response

Service Recovery Team (Operational) *(See Service BCP's for detail re plan's roles and responsibilities)*

- Determine who can invoke the Service Business Continuity Plan
- Determine appropriate response strategy, identifying which components of the recovery arrangements are to be activated under the circumstances
- Liaise with Comhairle Incident Team
- Appropriate stakeholder communication
- *Any other roles*

Site Recovery Team

- Damage assessment
- Liaise with emergency services
- Implement disaster recovery plans if necessary
- Facilitate loss adjuster
- Securing the site
- Salvage
- *Any other roles*

IT Recovery Team

- Damage assessment
- Implement disaster recovery plans if necessary
- Providing a restored technical environment so that services can access their systems & data
- Facilitate loss adjuster
- Securing the site and equipment
- Salvage
- *Any other roles*

8.0 Plan activation

In the event of a **major incident** there will be an organisation-wide invoking of Business Continuity Plans.

The following scenarios could constitute a major disruption at Comhairle wide level, i.e., may require strategic oversight:

- Danger to life
- Pandemic
- Extreme weather conditions leading to service disruption
- Raising of the national threat level
- Disruption to a critical **service** for 1 days +
- Major power outage or complete IT infrastructure failure
- Prolonged strike action
- Lost IT supporting a critical **service** for 1 day +
- Disruption to a non-critical **service** for 3 days +
- Loss of building

However, a **minor incident** may occur where individual services invoke their BCP.

The following scenarios could constitute a disruption at service level, i.e., may stretch resources beyond a normal operational resource and require tactical coordination:

- Adverse weather
- Disruption to a critical **activity** for 1 day +
- Loss of office space
- External event likely to cause disruption, i.e., strike
- Short-term power cut
- Loss of IT supporting a critical **activity** for 1 day +
- Disruption to a non-critical **activity** for 3 days +

Who? See Section 2 at the beginning of this document for who has the authority to declare a major incident and invoke this plan.

How? Call a meeting of the Corporate Management Team (see Section 10 Communications Strategy)

Notify the Comhairle Incident Team immediately if the plan is invoked

9.0 Incident Assessment Criteria

An incident assessment is useful for gathering the facts about an incident to inform subsequent decisions. If the answer to 2 or more questions is 'Yes' the incident is considered to be severe the Corporate Business Continuity Plan should be activated:

Incident Assessment Criteria	**No - Minor**	**Yes - Severe**
1. Does / will the incident require the emergency services to respond? E.g. fire, injuries, or potential criminal investigations		
2. Is the incident / disruption likely to last more than 24 hours or 1 working day?		
3. Does the incident affect more than 1 critical **service**?		
4. Is there – or is there likely to be **national** media interest?		
5. Is there likely to be any medium to long-term disruption to critical **services**?		
6. Does the incident pose significant reputational, financial or operational risks to the service or Comhairle?		

This assessment should be reviewed by Corporate Management Team as the incident goes on, and any changes communicated to the Comhairle Incident Team.

10.0 Communications Strategy

Corporate Management Team will meet at:	Committee Room 1
Alternative meeting location:	Committee Room 4
Frequency of meetings at outset:	

Communication with stakeholders is dealt with by the Incident Team and Recovery Teams.
Communication with the ResilienceDirect network is dealt with by the Incident Team.

11.0 Stand down process for the end of the incident

The following criteria:

- Critical **services** have now resumed to pre-incident levels, or as close to pre-incident as is reasonably possible
- A log of the ongoing issues and risks has been handed over to ***relevant operational teams***
- A post incident report has been issued
- Corporate Management Team agree to stand down

Table 1 – Generic Response to an incident (which causes a disruption to business activities)

Guidelines	Description	Tools
1. Evacuate the workspace (if necessary)	a) Follow Emergency Response Evacuation Plan	**Evacuation Plan**
2. Alert the most senior manager on site (if they are not aware)	a) Continue to issue instructions to emergency response personnel b) Assess the incident and potential disruption c) Decide if Business Continuity Plan should be activated	**Business Continuity Plan**
3. Alert all members of the Service Recovery Team and Comhairle Incident Team	a) Meet at a suitable location b) Start a 'decision log' c) Gather information about the incident from as many sources as necessary d) Assess the impact of the incident and how the situation is likely to evolve e) Notify key stakeholders f) Review Service Recovery Team roles and responsibilities	**Decision Log template** (see Incident Management Team Shared folder) Service Recovery Team roles and responsibilities
4. Immediate Response Actions	a) Develop Action Plan b) Appoint 1 person to liaise with Comhairle Incident Team and other key stakeholders c) Ensure safety of staff d) Ensure safety of clients / customers / communities e) Ensure protection of the environment f) Ensure protection of organisational assets	**Action Plan template** (see Incident Management Team Shared folder)
5. Assessment	a) Assess impact on operation b) Assess impact on organisational assets c) Assess what resources are necessary to return to normal operations	**Resource Requirement Checklist** (Service BCPs) **Specific Response Plan** (Appendix A, Incident Management Team Shared folder and Service BCPs)
6. Communications	a) Develop a communications strategy at an operational level, i.e., staff and operational stakeholders	

	- Identify who the key stakeholders are, and who will communicate with them - Notify Comhairle Incident Team - Communicate with staff regularly - Communicate with internal departments (BIA)	
7. Normal Operations	a) Develop plan to return to normal operations as quickly as possible - Agree on priorities to be recovered (critical activities) - Identify and order equipment needed - Review raw materials and stock held - Liaise with internal departments - Communicate with staff - Obtain authorisation for emergency expenditure - Ensure compliance with regulations in operation	
8. End of incident declaration	a) Authorise return to normal operations b) Monitor ongoing response and performance of workspace c) Maintain communications strategy for staff and operational stakeholders as long as necessary	
9. Continuous Learning	a) Hold post-incident debrief b) Record Lessons Learned and update Business Continuity Plan with Lessons Learned	**Lessons Learned Log** (see Incident Management Team Shared folder) **Business Continuity Plan**

There are a range of specific scenarios that would require a response. Some of these are outlined below. This section highlights the strategies that could be considered. The Business Continuity Risk Assessment should be used here as it determines the higher-level threats faced by critical activities and consideration should be given to developing these into **'Specific Response Plans'** outlining the response to the potential incident.

Appendix A contains a **'Specific Response Plan'** example.

Table 2 – Specific Actions

Threat	Actions / Options	Tools
1. Supply Chain disruption	- Order extra supplies from an alternative supplier, ensuring quality is good - Prioritise limited supplies on services for essential customers - Offer customers alternative products we have in surplus - Bring in supplies from other plants that have higher stock levels	**Specific Response Plan**
2. Loss of IT or Communications	- Bring in backup IT equipment and restore data and systems from backups - Relocate minimum staff / operations to other sites (see BIA) - See options below - **3. Loss of Workspace** in extreme circumstances	**Specific Response Plan**
3. Loss of Workspace or Access to Workspace Possible Causes: • Fire • Flood • Building collapse • Extreme weather • Contamination • Closed by administration • Serious Health & Safety incident	- Relocate to other workspaces where possible - Relocate to alternative 3rd party premises using salvaged equipment, and buying in new equipment where necessary - Outsource operation to 3rd party supplier – with agreement from customers - Relocate operation to another site by transporting specialist equipment	**Specific Response Plan**
4. Loss of Power Possible Causes: • Failure of energy provider infrastructure • Failure of key equipment	- Mobile generators could supplement power from the grid - Reduce operations by moving some operations elsewhere - Delay some operations until 100% power is restored and advise customers - Offer an alternative service to some customers	**Specific Response Plan**

5. Loss of Water	- Stop operation until water supply restored - Relocate some operations to other sites - Bring in mobile water tankers - Use portaloos	**Specific Response Plan**
6. Loss of Key Equipment	- Hire equipment - Buy 2nd hand equipment - Order new equipment - 'Borrow' equipment from another plant - Transfer operation to another plant that does not have equipment - Outsource some operation to a 3rd party - Reduce services to essential customers / most vulnerable - Stop service / operation	**Specific Response Plan**
7. Loss of People / Staff Possible Causes: • Pandemic • Strike • Illness • Workers unable to travel due to extreme weather • Specialists skills lost	- Consider which tasks or activities can be stopped or reduced: workers can then be switched into other roles if they are trained to do them - Use process maps and documentation to allow staff to undertake roles with which they are unfamiliar - Ensure all employee information is up-to-date, and includes home email address, home telephone and mobile telephone numbers wherever possible - Identify temporary staff or agencies that can supply staff at short notice - Consider increasing operation through overtime, extra shifts or weekend working - Consider if some operations can be reallocated to other sites - Consider if some operations can be outsourced to a 3rd party	**Specific Response Plan**

Appendix A – Example 'Specific Response Plan' for a Fire

No	Actions	Notes	Priority / Timing	Accountability	Complete
1	Initiate fire evacuation plan		High	Service Manager	
2	Hand site over to fire brigade		High	Premises Manager	
3	Convene Service Recovery Team at appropriate command centre location		High		
4	Activate Business Continuity Plan		High		
5	Contact Comhairle Incident Team to advise		High		
6	Assign someone to liaise with Fire Brigade		High		
7	Make assessment of likely duration of incident and impact on operations		High		
8	Decide if staff should remain on site / go to alternative site / be sent home		High		
9	Review situation with clients / customers / communities		High		
10	Complete Action Plan		High		

Specific Response Plans are held in the shared Incident Management Team folder or see Service BCPs

The Critical Services Priority list is held here: Business Continuity Management