Business Continuity Management Policy

June 2025

Version: 2

City of Newcastle

Table of Contents

Part A - Preliminary

1 Purpose

1.1 The purpose of this Policy outlines City of Newcastle's (CN) Business Continuity Management (BCM) Framework (the Framework) and measures that assist to:

a) Minimise the impact of Incidents, Disruptions and emergencies

b) Safeguard CN's critical services and functions

c) Support the effective return to normal operations and build organisational resilience through enhancing capabilities.

1.2 The Framework, as outlined in this Policy, has been established to ensure that CN can continue to deliver critical business functions if an Incident, Disruption or emergency Disruption impacts CN’s business as usual capabilities.

2 Context

2.1 This Policy supports CN's compliance with Office of Local Government (OLG) *Guidelines for Risk Management and Internal Audit for Local Government in NSW*, with respect to Audit Risk & Improvement Committee responsibilities around business continuity management. CN's approach and this Policy have been developed in consideration of ISO 22301 on business continuity and the high-level framework structure to apply.

3 Scope

3.1 This Policy applies to all CN employees, contractors, volunteers and incorporates business continuity responsibility into all areas on CN's operations.

3.2 It does not apply to external agencies that may assist in a business continuity event (an Incident, Disruption or emergency that impacts CN operations).

4 Principles

4.1 CN commits itself to the following objectives:

Accountability and transparency – This Policy provides a framework outlining the approach taken by CN in managing its business continuity risks and the accountabilities related to it.

An all hazards approach – BCM response strategies will focus on the outcome and management of the Disruption rather than the cause. Alternative operating arrangements will be developed to address loss or reduce access to buildings or infrastructure, information and communications, technology and/or impact to employees.

Collaboration and productive relationships – CN will provide clarity around the roles and responsibilities of relevant employees during a crisis or emergency, with structured escalation and communication pathways to encourage action and conversation in the planning, response and recovery stages.

Culture of continuous improvement – CN will review and test the Framework to build awareness, resilience and capability. Further, CN will allow for clear and effective de-briefs post event and will provide consistency to support shared learnings and instil a system of continuous improvement.

Health, wellbeing and safety – CN’s priority will always be the immediate and ongoing safety of all CN employees, contractors, and volunteers as well as the community.

Promotion of local decision making – The Framework will provide CN with a structure to prepare, plan, respond and recover. This will support employees to make informed decisions with transparency and allow decisions to be made at the appropriate level to address emerging needs.

Scalable and adaptable – CN will utilise the Framework to manage any Incident, Disruption or emergency regardless of the severity, size or complexity, tailoring its approach, ensuring appropriate capabilities are available and prepared, supporting flexibility and agility in CN's response.

Part B - Policy Statement

5 Objectives

5.1 The objectives of the Framework are to ensure that during an Incident, Disruption or emergency, CN:

a) Prioritises key resources necessary to operate critical business processes

b) Maintains employee, stakeholder and community contact and confidence

c) Fulfils its legislative compliance responsibilities

d) Appropriately controls and monitors extraordinary expenditure resulting from the Incident, Disruption or emergency

e) Controls risk priority areas

f) Safeguards the reputation of CN and the local government area.

6 Business Continuity Management Framework

6.1 CN's Framework comprises of this Policy along with various support plans, assessments and procedures at a functional and site level. More specific details around roles and responsibilities during an Incident or Disruption, are outlined in these plans. These are general guidance documents maintained by the respective Service Unit, and include:

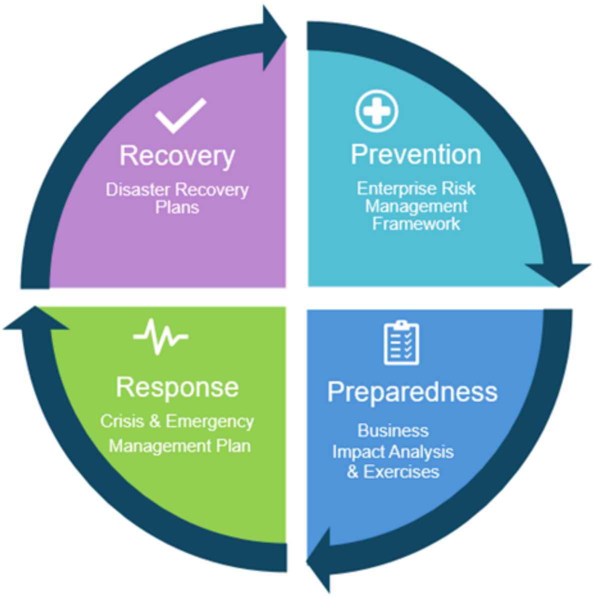
- Enterprise Risk Management Framework
- Business Continuity Plan (BCP)
- Supporting Business Impact Analyses (BIAs)
- Crisis and Emergency Management Plan (CEMP)
- IT Disaster Recovery Plan (including the Cyber Incident Response Plan)
- Recovery Plans
- Site Emergency Response.

The Framework is an integral component of CN's corporate governance framework.

6.2 The following diagram summarises the practical operation of the Framework:

CN utilises the Prevention, Preparedness, Response and Recovery model in its approach to its business continuity planning process. The below diagram outlines this circular model, which promotes a process of continuous improvement.

Business Continuity Process


Recovery
Disaster Recovery Plans
Prevention
Enterprise Risk Management Framework
Response
Crisis & Emergency Management Plan
Preparedness
Business Impact Analysis & Exercises

i. **Prevention:** Outlines the actions CN has taken in advance to prevent events or mitigate them. The Enterprise Risk Management Framework outlines the risk architecture, appetite and tolerance for risks, along with its approach to managing risks including business continuity. Controls are documented on how CN mitigates its business continuity risk and the responsibilities for these

ii. **Preparedness:** CN conducts various business impact analysis to identify critical service functions to be restored during an event. This maps outs resourcing, priorities and timeframes required for critical functions to recommence. In addition, the overarching BCP outlines the holistic approach undertaken to planning and preparing for an event. Education and training on such plans through exercises with the EOC/IMT assist in CN's preparation for events and build confidence in managing them

iii. **Response:** Requires CN's assistance or intervention during or immediately after an event to protect lives and community assets. This is addressed by various site response plans and procedures, along with organisational decision making through the Crisis & Emergency Management Plan and the Cyber Incident Response Plan

iv. **Recovery:** Relates to CN's coordinated process of supporting the community and reconstruction of its physical infrastructure. CN's IT Disaster Recovery Plan and site emergency response and recovery plans assist to guide service units in managing this phase.

6.3 The Framework provides for:

- A scalable approach to activating the BCM processes, depending upon the complexity and severity of an Incident or Disruption. This shall be activated in line with the appropriate triggers outlined within the CEMP
- The appropriate level of resources to ensure that BCP initiatives and actions can be implemented
- A practical approach which is flexible and easily engaged in the event of an Incident, Disruption or emergency.

7 Review

7.1 The Framework:

- Is reviewed and updated where necessary, and at least every three years. Tested annually in conjunction with the CEMP and validated through exercises and scenarios for employee training and evaluation purposes

- Mandates participation of representatives from each Directorate in crisis and emergency management and in business continuity matters to ensure that key personnel can perform competently during a major Incident, Disruption or emergency.

A review of the BCM Framework will form part of the Enterprise Risk Management reporting responsibilities to both the Governance and Risk (Executive) Committee and the Audit Risk and Improvement Committee.

Part C - Roles and Responsibilities

POSITION	RESPONSIBILITY
CEO	Activation of the BCP and CEMP. Leading and championing a culture of responsible BCM.
Executive Directors and Executive Managers	Being the custodians of BCM capability within their Directorate / Service Unit, including the development, maintenance and validation of their specific BCP information (including Business Recovery Plans and BIA's) and the management of any risks related to BCM. Developing and supporting a culture of responsible BCM within their Directorate / Service Unit. Allocating resources on activation of BCP within Directorate or on the activation of the CEMP (each Directorate must allocate resources for training and on activation). Regularly reviewing Directorate / Service Unit activities to ensure that critical processes and systems are addressed through periodic business impact analysis activities. Enacting BCP where appropriate.
Legal and Governance	Overseeing and monitoring the development, implementation, resourcing and maintenance of the Framework. Provision of training opportunities for persons responding to Incidents and emergencies. Co-ordination and facilitation of an annual test exercise. Reporting to the Governance and Risk (Executive) Committee (GREC) on the status and effectiveness of the Framework. Ensuring that there is an integrated and co-ordinated approach to risk management, business continuity and emergency management.
Chief Information Officer	Development, testing and activation of the IT Disaster Recovery Plan and Cyber Incident Response Plan (CIRP).
Audit Risk and Improvement Committee	Effectiveness of business continuity arrangements, including business continuity plans, disaster recovery plans and the periodic testing of these plans as prescribed in their Charter.
All employees	All employees should be aware of BCM Framework and Business Continuity Planning.
Third party dependencies	All planning, negotiating and managing of outsourced agreements with third parties that provide critical service, will comply with CN's risk tolerance, including addressing continuity planning. Critical external service providers must be required to demonstrate they have adequate business continuity arrangements in place (or bridging arrangements) as part of the contracting or procurement process.

Annexure A - Definitions

Business Continuity Management (BCM) means the process of putting in place plans, procedures and guidelines to support efforts in maintaining continuity of business during a disruptive or emergency event.

Business Continuity Plan (BCP) means a documented collection of strategies and actions for use by CN in a disruptive event to enable a critical business function to continue to deliver its services to an acceptable minimum level and transition to normal operations.

Business Impact Analysis (BIA) means a risk-based assessment used to identify the service units' critical systems and business processes.

Business Recovery Plans - provide the information for the service units to recover their critical processes.

CEO means Chief Executive Officer of the City of Newcastle and includes their delegate or authorised representative.

References to the Chief Executive Officer are references to the General Manager appointed under the Local Government Act 1993 (NSW).

City of Newcastle (CN) means Newcastle City Council.

CN Staff means employees of CN (including full time, part time, fixed term and casual) or Specific Talent Contractor who is engaged under a CN position description.

Disruption means anticipated or unanticipated event that interrupts normal functions, operations, or processes (e.g. severe weather, political or labour unrest, utility outage, criminal/terrorist attack, technology failure, or earthquake)

Incident means an event that if not handled in an appropriate manner, the situation can escalate into a Disruption or emergency that negatively impacts CN's operations, reputation, or community.

Annexure B - Policy Authorisations

This Policy Authorisation may be updated and amended by the CEO from time to time.

In accordance with section 378 of the *Local Government Act 1993*, the Chief Executive Officer delegates the following functions to the positions listed:

Title of Authorisation	Description of Authorisation	Position Number and Title
Nil		

Document Control

Policy Title:	Business Continuity Management Policy
Audience:	CN Staff
Service Unit:	Legal and Governance
Policy Owner:	Executive Manager Legal and Governance
Policy Writer:	Enterprise Risk Manager
Approved by:	CEO
Date Approved:	18 June 2025
Commencement Date:	18 June 2025
Next Scheduled Review Date:	30 April 2028
Termination Date:	30 April 2029
Version:	Version 2
Required on Website:	No
Key Words:	Business Continuity, Business Continuity Framework, Risk Management, Business Continuity Plan, Incident, Crisis and Emergency Management, Business Impact Analysis

Related Document Information, Standards & References

Related Legislation:	Nil
Related Policies (Council & Internal):	Enterprise Risk Management Policy
Related Procedures, Guidelines, Forms or documents:	OLG Guidelines for Risk Management and Internal Audit for Local Government in NSW Business Continuity Plan IT Disaster Recovery Plan Crisis & Emergency Management Plan
Standards, Codes or other references:	Nil

Relevant Newcastle 2040 Theme/s

Term / Abbreviation
Achieving Together

Version History

Version No - Date Approved - ECM
Version 1 - Approved 30 July 2021 - ECM: 7131016