

BUSINESS CONTINUITY MANAGEMENT POLICY

POLICY NO:	POL/487
VERSION:	June 2018 D18/162535
SHORT DESCRIPTION:	To detail the Business Continuity Management Framework that will support an effective response to a significant business disruption to 'Business As Usual'.
RELEVANT TO:	All employees
RESPONSIBLE OFFICER:	Executive Manager People and Governances
RESPONSIBLE OFFICE:	Risk Management and Assurance
APPROVED BY:	Risk Management Committee on 20 June 2018 Adopted by Council on 28 August 2018
NEXT SCHEDULED REVIEW DATE:	June 2020
RELATED DOCUMENTS:	Crisis Management Response and Recovery Plans Directorate Critical Services Sub Plans Directorate Critical Services Business Impact Analysis Spreadsheets IT Disaster Recovery Plan Risk Management Policy

1. POLICY PURPOSE

The purpose of this Policy is to outline Manningham City Council's (MCC) Business Continuity Management (BCM) framework, including key fundamentals such as:

- Objectives and principles of BCM
- The BCM framework
- Critical Service risk assessment and Business Impact Analysis process
- Roles and responsibilities
- Plan testing and reporting.

For clarity, this policy does not create an additional reporting framework. BCM is a control or treatment to risks that impact the organisation's continuity. As such, reporting on the framework will be through the Risk Management Framework.

MCC is committed to managing disruption-related risk effectively. As such, the policy considers relevant BCM standards such as AS/NZS 5050:2010 Australian/New Zealand Standard Business continuity—Managing disruption-related risk, HB 292-2006 A Practitioners Guide to Business Continuity Management, Business Continuity Management – Building Resilience in Public Sector Entities, better practice guide, 2009 and Business Continuity Institute Best Practice Guidelines.

2. BCM OBJECTIVES AND PRINCIPLES

“Contingent capacity and plans enable management to quickly focus on stabilising the situation and maintaining or resuming the most critical functions while still working in a planned way towards eventual restoration of routine operations and full achievement of objectives”. AS/NZS 5050:2010

The benefits of having an effective Business Continuity Management framework include:

- Demonstrating organisational commitment and capability to manage BCM risks.
- Helping to ensure continuity of critical services to customers and to protect brand and reputation
- Helping to identify and manage current and future threats to the business
- Identifying regulatory and contractual requirements and obligations that are required to be delivered during a crisis
- Minimising downtime during incidents and improve recovery time
- Demonstrating resilience to customers, suppliers and the Council.

The objectives of MCC’s BCM Framework is to help reduce the occurrence and scale of events that could cause a “major” or “catastrophic” disruption as well as equipping the organisation with the capacity to:

- Have a clear transparent and systematic approach to the activation of the Crisis Management Plan and delegation of control
- Stabilise any disruptive event as soon as possible
- Continue and/or quickly resume those services/operations that are most critical to the organisation’s objectives and legislative obligations
- Minimise the impact on our people, our residents and reputation
- Provide a structured and consistent response to an unexpected crisis or anticipated disruptive event, from Crisis Management Team to operational level
- Expedite a return to ‘Business As Usual’ operations and a full recovery.
- Provide assurance to the Audit Committee and Council that a process of rigorous development and testing has been applied to BCM planning
- Ensure external communication to clients and stakeholders is maintained or promptly reinstated during a crisis.

Crucially, the BCM Framework needs to:

- Be sustainable
- Consider incident activation, plan activation, managing the incident and plan deactivation
- Have clearly defined roles and responsibilities to enable officers to act effectively and timely, with clear reporting processes that facilitate appropriate command and control oversight and management of the incident
- Provide structure regarding the management of an incident at both the strategic and operational levels
- Identify critical services and their dependencies
- Undertake regular BCM testing and training for key staff. Testing should validate the appropriateness of plans, increase capability and enable continuous improvement.

3. Emergency Management

The council could be impacted by two types of emergency events. These are detailed below:

- Community based emergency - Municipal Emergency Management Plan
- Council services/assets based crisis - Crisis Management Plan.

Community Based Emergency

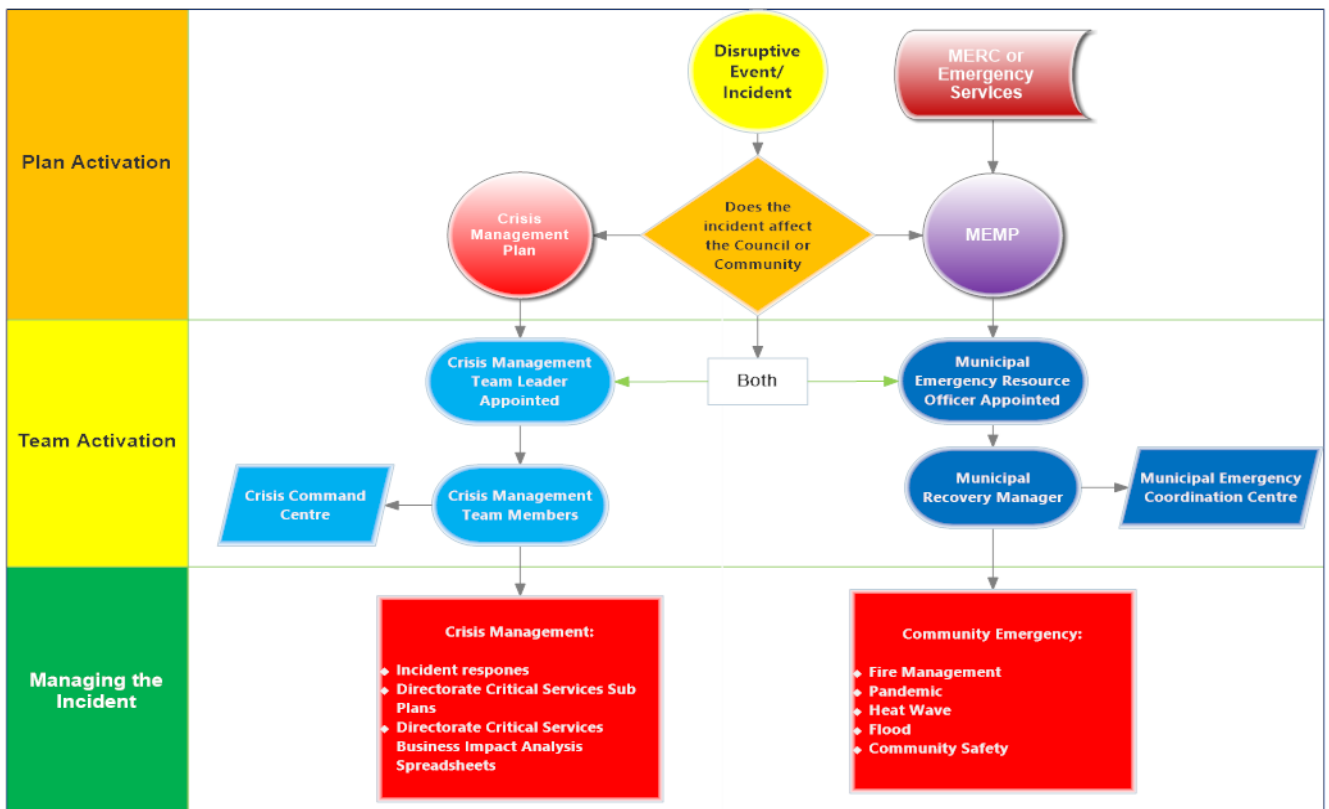
These events usually involve managing a community emergency response, i.e. flood/fire evacuation and coordination with other authorities. In the case of a community based emergency, the Municipal Emergency Management Plan (MEMP) would be activated in accordance with the Emergency Management Act. These incidents are usually managed by Emergency Services/Agencies in the first instance, before having Council involvement through the Municipal Emergency Coordinator (MERO) or nominated Municipal Recovery Manager. This policy does not address this type of event but demonstrates the interconnectedness, plans for communication and protocols.

Council Services/Assets Based Crisis

These incidents impact the Council's ability to deliver critical services. Whilst MCC's BCM framework is part of the Council's overall emergency management framework, its application is directed to a Council based incident. In these circumstances, the Crisis Management Plan would be activated.

It is understood that if the MEMP and Crisis Management Plan are activated together, resources/assets are to be prioritised to implementing the MEMP (under the control of the MERO) using the asset allocation principle of "Health and well-being of the Community is the first priority".

Below is an overview of the Councils emergency management framework.



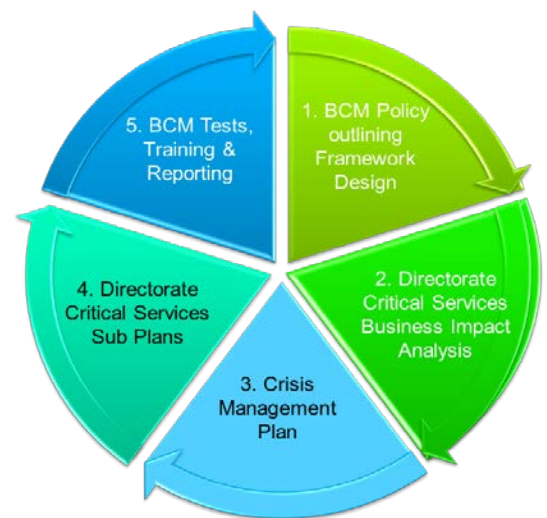
4. BUSINESS CONTINUITY MANAGEMENT FRAMEWORK

Australian National Audit Office states “Business continuity management is an essential component of good public governance. It is part of an entity’s overall approach to effective risk management and should be closely aligned to the entity’s incident management, emergency response management and IT disaster recovery.”

The key element of the BCM framework are:

1. **BCM Policy** – details the elements of the BCM framework
2. Directorate ‘Critical Services’ risk assessment and **Business Impact Analysis Spreadsheet** (detailing the dependencies required to deliver critical services).
3. **Crisis Management Response & Recovery Plans** – generic response plan that covers incident assessment, plan activation process, managing the incident and team deactivation.

The Plans outlines Crisis Management Team roles, responsibilities and contact details. Includes incident planning and management templates, crisis control centre and communications centre details, as well as initial response checklists.



4. Directorate Critical Services Sub Plans

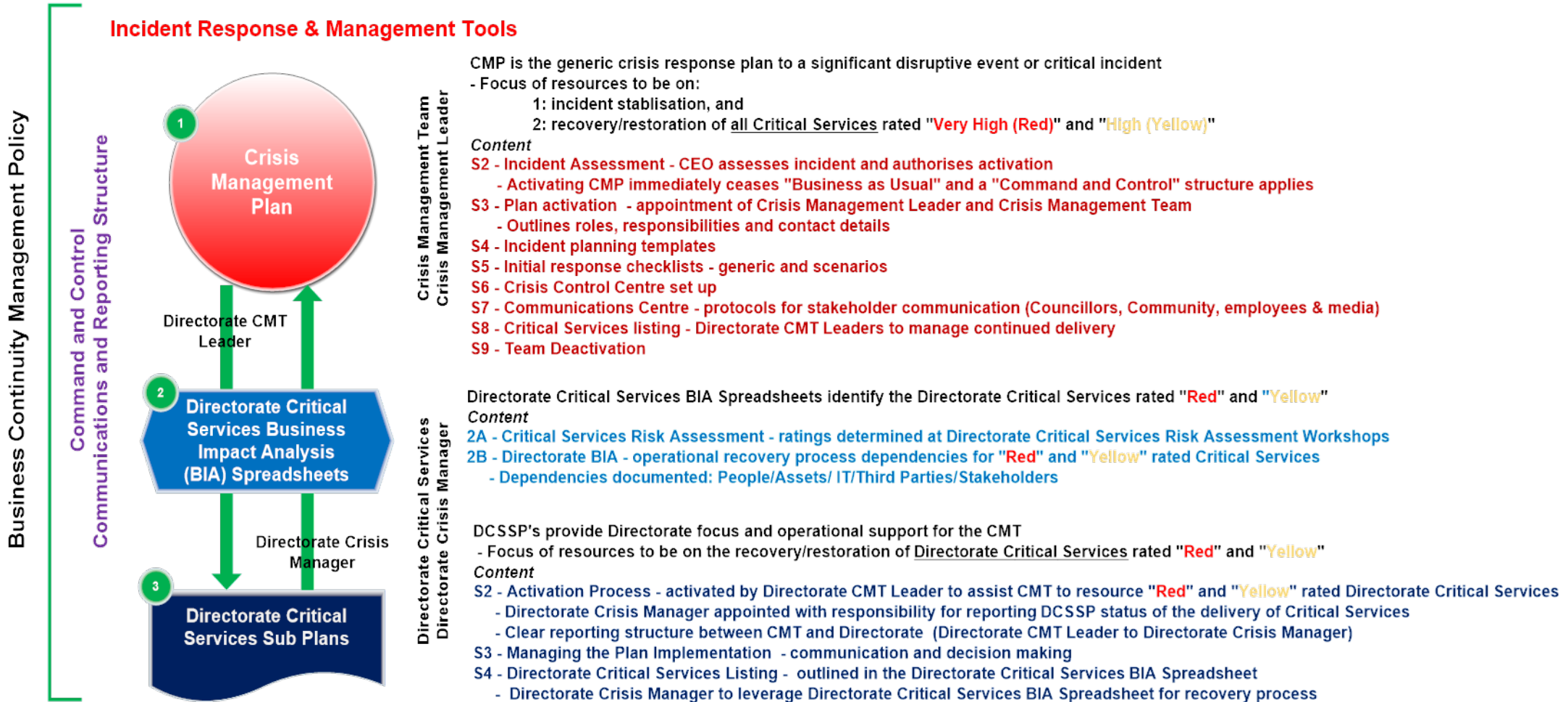
These Directorate plans list each Directorate’s Critical Services identified in the Directorate Critical Services Business Impact Analysis Spreadsheet. The plans provides structure at the operational level with regards to recovering/restoring “High” and “Very High” rated critical services.

The Directorate Critical Services Sub Plans may be supported by **Service Unit Relief & Recovery Sub Plans**. ie. Citizen Connect, Aged and Disability Support Services.

5. BCM Tests, Training and Reporting – annual testing is anticipated together with reporting in accordance with the Local Government Performance Reporting Framework indicators.

Manningham's Business Continuity Management Framework Summary

The framework is designed to assist the response to a significant disruptive event or critical incident that could have a "major" or "catastrophic" impact.



5. Critical Service Risk Assessment and Business Impact Analysis

During an incident resource focus need to be prioritised based on:

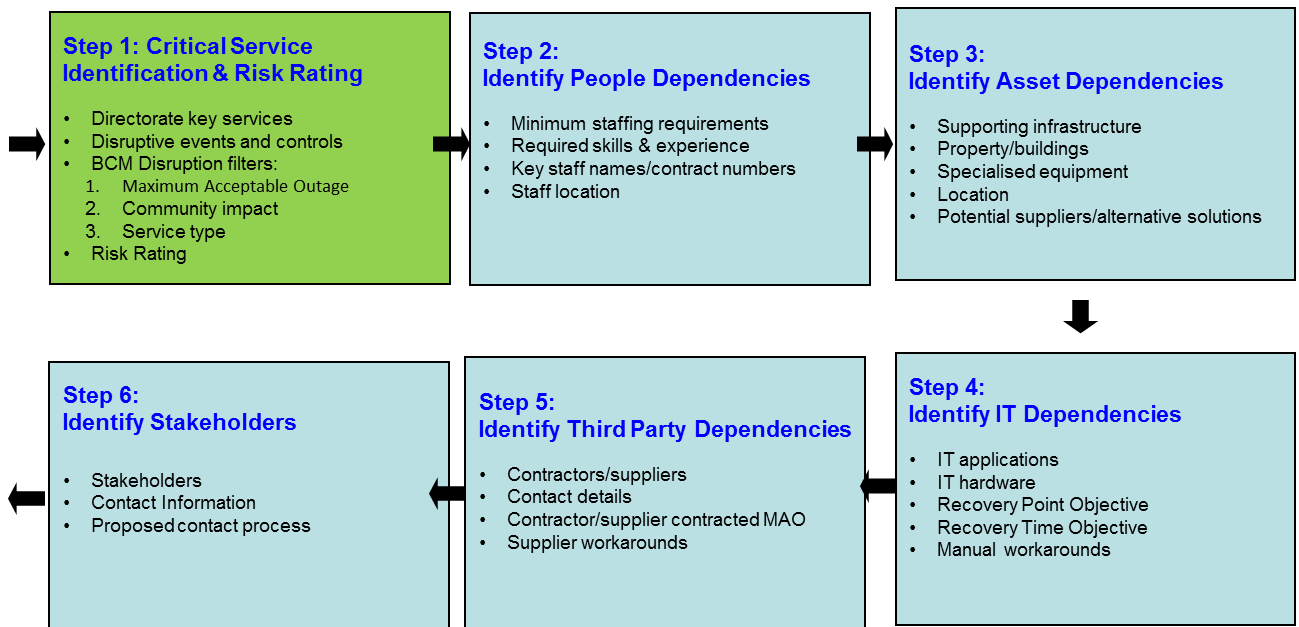
1. Incident stabilisation, and
2. Recovery/restoration of critical services rated “High” and “Very High”.

Critical Services are services that if not delivered, would have a major or possibly catastrophic impact on council’s reputation, client health, legislative or contract compliance, service delivery, financial performance and public health and safety. During an incident, Council must continue to deliver or quickly recover capabilities to deliver, Critical Services.

As such each Directorate shall undertake a Critical Services risk assessment to identify its ‘Critical Services’. The assessment process is detailed in the Directorate Critical Services Workshop Guidance Manual and should be recorded in the Business Impact Analysis Workbook.

Those services rated High or Very High will be considered ‘Critical Services’ and will require a Business Impact Analysis assessment. The Business Impact Analysis will identify service delivery procedures/ workflow maps/process manuals and the service dependencies needed to deliver a minimal service, including people, assets, IT, third parties and stakeholders.

The six step methodology adopted is as follows:



Outcomes from the Business Impact Analysis should be documented in Directorate Critical Services Business Impact Analysis Spreadsheet and feed into the Directorate Critical Services Sub Plans.

6. ROLES AND RESPONSIBILITIES

The development of a suitable structure to ensure the appropriate oversight and accountability in managing an incident is critical. MCC has authorised the following levels of responsibility:

Council

- Approve the Business Continuity Management Policy.
- During an incident where the Crisis Management Plan has been activated, Management will provide the Councillors with timely communications.
- Where considered appropriate, the Mayor may be required to provide communications to stakeholders.

Audit Committee

- Consider the BCM Policy for Council approval.
- Monitor the management of Council's strategic risk controls

Risk Management Committee

- Review the BCM Policy every two years
- Monitor the annual testing, reporting and update of the BCM Framework

Chief Executive Officer (CEO)

- Responsible for the BCM Framework within MCC.
- Activate/deactivate the Crisis Management Plan.
- Appoint the Crisis Management Leader.
- Agree incident recovery objectives, incident authorisation arrangements and endorse major Crisis Management Team recommendations and decisions.
- Advise the Mayor, Councillors and Government as appropriate, on the status of an incident.
- Ensure appropriate reporting to the Audit Committee and Council.

Crisis Management Team Leader

- Lead the Response and Recovery process to restore business operations and delivery of services.
- Initiate Council's business continuity response.
- Appoint the Crisis Management Team and agree roles and responsibilities.
- Approve the Crisis Management Team Crisis Command Centre's location.
- Liaise with MERO if the MEMP activated.
- Perform preliminary event analysis and determine key strategic issues and recovery objectives.
- Chair the Crisis Management Team meetings.
- Provide the Crisis Management Team with directions.
- Report to the CEO on major decisions.

Crisis Management Response and Recovery Team

- Assist the Crisis Management Team (CMT) Leader with the recovery and plan activations.
- Undertake designated roles, as per role cards or as directed by CMT Leader.
- Determine resource requirements to fulfil their responsibilities.
- Provide regular status information to the CMT leader.
- Provide communications to internal and external stakeholders (via the Community Relations and Engagement Response Leader).

Directorate Crisis Manager

- Upon request by Response and Recovery Management Leaders, activate Directorate Critical Services Sub Plan.
- Manage the implementation of the Directorate Critical Services Sub Plan, leveraging the Directorate Services Business Impact Analysis Spreadsheet.
- Report the status to the Directorate Crisis Management Team Leader.

Staff

- Assist the Crisis Management Team or Directorate Crisis Manager where requested.
- Unless specifically requested, do not communicate to the public.
- Work with their Directorate Crisis Manager to activate Directorate Critical Service Sub Plans and Service Unit Relief & Recovery Sub Plans.
- Work at locations determined by the Crisis Management Team.

More specific details of the Crisis Management Team roles and responsibilities is set out in the Crisis Management Plan.

7. TESTING AND TRAINING

It is important that the Crisis Management Team members maintain an intimate knowledge of their individual role. Team members and their relevant alternates must have a working knowledge of the BCM framework and relevant plans.

BCM test exercises will be conducted at least annually. These exercises should ensure BCM plans are up-to-date and remain relevant. Tests should be formally conducted and consider governance elements such as the development of detailed test plans, pre-test briefing sessions, testing protocols including issues logging, Recovery Time Objective recording and appropriateness of plan/workbook information. Post each test, debrief sessions should occur with participants to evaluate what worked and what could be further improved. Plans should then be updated and the test results reported to the Risk Committee and Audit Committee.

8. REPORTING

The follow is an outline of the BCM reporting structure:

1. Local Government Better Practice Guide Plan requires Management to confirm that they have a Business Continuity Plan setting out the actions that will be taken to ensure that key services continue to operate in the event of a disaster and details of the date of operation. This needs to be reported in the annual report and to the Department of Environment, Land, Water and Planning.
2. Directors with BCM risks will need to review their Directorate Critical Services Sub Plan and Directorate Services Business Impact Analysis Spreadsheet annually
3. As Business Continuity is a strategic risk, the CEO will need to report to the Audit Committee on the treatment plans, which includes the monitoring of the BCM framework
4. Annual review of the Crisis Management Plan to be managed by the Strategic Risk and Assurance Advisor.

9. KEY DEFINITIONS

Term	Definition
Crisis Management Plan Activation	Process whereby the CEO authorised the activation of the Crisis Management Plan. Activation causes Council's "Business as Usual" operations to cease and is replaced with a strong "Command and Control" communication and reporting structure.
Business As Usual	Normal operations without any significant constraints.
Business Continuity Management (BCM)	A holistic management process that identifies potential threats and impacts to business operations and which provides a framework for building organisational resilience and capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
Business Impact Analysis (BIA)	The process that quantifies the disruptive impact of a given incident or disruption and identifies the infrastructure and resources required to enable the organisation to operate at the minimum accepted level.
Call Tree	Details who contacts which member of the Crisis Management Team upon activation.
Crisis Management	What you do before, during and after an incident/event/crisis/emergency.
Crisis Management Response Plan	A generic response plan to assist Management with the strategic coordination and management of a crisis event. Covers incident assessment, plan activation process, managing the crisis event and team deactivation.
Crisis Management Plan Resource Recovery	A companion guidance document to the Crisis Management Response Plan following activation. It provides a structured set of tasks, including role cards and templates for the Crisis Management Recovery Team to restore a critical service.
Critical Service	A service that is rated High or Very High and if not delivered, would have a major or catastrophic impact on Council's reputation, client health, legislative or contract compliance, service delivery, financial performance and public health and safety.
Disruption filters	Risk assessment filters used to determine the criticality of a service. Include Maximum Acceptable Outage (48 hours, 7 days or 30+ days), community impact (high dependency, high volume or low volume) and service type (core internal, contracted or statutory).
Disruptive event	An incident such as loss of public infrastructure, loss of staff, loss of building, loss of fuel and utilities, loss of IT and loss of telecommunications.
Incident Assessment	Process of identifying and rating the incident severity. The Incident Severity Table detailed in the CMP provides a guide for assessing an incident.
IT Disaster Recovery Plan (IT DRP)	Those BCM activities associated with the continuing, availability and restoration of IT infrastructure, including systems and applications.
Maximum Acceptable Outage (MAO)	Maximum period of time that an organisation can tolerate the disruption of a critical service.
Plan Activation Process	Process of declaring a crisis and appointment of the Crisis Management Leader and Crisis Management Team.
Recovery Point Objective (RPO)	With respect to the recovery of electronic data (system or application data), it relates to the last point in time prior to the business disruption, that the data was restored or backed up. This data will need to be re-entered once IT systems have been recovered.
Recovery Time Objective (RTO)	A target time period set for resumption of service delivery, recovery of an IT system or application, or resumption of performance of a service after a business disruption.
Risk treatment	Process of selection and implementation of measures to modify risk. BCM plans are risk treatments and become risk controls once finalised and tested.