BUSINESS CONTINUITY MANAGEMENT POLICY

ECM DSID Number:	4246620
First Issued / Approved:	14 December 2021
Last Reviewed:	14 December 2021
	C141221/2505
Next Review:	14 December 2024
Responsible Officer:	Manager Strategy and Governance
Date Placed on Webpage/ Intranet:	24 December 2021

1. PREAMBLE

Business Continuity Management (BCM) is a holistic management process that identifies potential threats to an organisation and the impacts to business operations if those threats arise. BCM builds organisational resilience and capability to effectively respond to events in order to safeguard the interests of its key stakeholders, reputation, brand and value-creating activities.

Council aims to conduct its operations with the highest regard for the wellbeing of its people, while maintaining the highest quality service to its customers and protecting its business and the environment. If a disruptive event occurs, the objective of BCM is to:

- minimise risks to the health and safety of employees, contactors, customers and the public, and
- minimise the period of the disruption and maximise the speed of recovery to normal business activities for all stakeholders.

1.1 Background

The City of Holdfast Bay (the Council) is committed to adopting a strategic, consistent and structured approach to BCM in line with the principles of ISO22301:2012 Business Continuity Management Systems.

The Council is committed to excellence in BCM and is committed to continuously improving its practices.

The Council acknowledges that BCM is essential for sound strategic, financial and operational planning and the achievement of the Council's objectives.

1.2 Purpose

Council is obliged to ensure that critical business functions continue after a business interruption. The purpose of this Policy is to outline the Council's principles for BCM, the approach to be taken to implement BCM and who has responsibility for activities within the program.

1.3 Scope

This policy applies to all of Council operations, including Alwyndor.

Council has developed plans, taking into consideration reasonably foreseeable risks and their potential impact on achievement of Council objectives. BCM has two key elements: Crisis Management and Business Continuity.

The BCM lifecycle is depicted below, as per ISO 22301:2012:

Council has identified these five steps to build, manage and maintain a robust BCM system.

The Council supports BCM practices and encourages and empowers staff in managing BCM in order to protect employees, contractors, clients and assets against reasonably foreseeable BCM risks within the boundaries of the Council's operations.

Emergency Management is managed by the Emergency Management Operations Manual and site-specific Workplace Emergency and Evacuation Plans.

BCM is supported by Council's Risk Management Policy and Risk Management Framework.

1.4 Strategic Reference

Culture: Supporting excellent, efficient operations

2. PRINCIPLES

2.1 Operation and Planning Control

Clear roles and responsibilities underpin BCM. Strategy and Governance lead the BCM program, including:

- communicating the importance of effective BCM and promoting continuous improvement,
- integrating BCM into the organisation's business processes,
- review the organisation's BCM processes and plans biennially,
- coordinate formal approval of all plans by the Senior Leadership Team.

Roles and responsibilities are articulated via the relevant plans.

2.2 Business Impact Assessments

In order to understand the business continuity risks that affect Council and the impact of these on the business, a biennial business impact analysis (BIA) will be undertaken.

BIA informs priorities and requirements for business continuity management and enables Council to prioritise the resumption of activities that support services, determining the following for each business function:

- Maximum Acceptable Outage (MAO) - The Maximum Acceptable Outage (MAO) is defined to be the time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity to become unacceptable (ISO 22301:2012).
- Recovery Time Objective (RTO) - The period of time following an incident within which an IT product or service must be resumed or recovered (ISO 22301:2012).
- Recovery Point Objective (RPO) - The point to which information used by an activity must be restored to enable the activity to operate on resumption (ISO 22301:2012).

The BIA must be refreshed after any significant change in Council, or at least every two years. This refresh should consider whether the criticality of any current business function has changed or whether new business functions exist that require a detailed BIA to be performed.

To understand the criticality of a business function, the following criticality matrix will be used. To determine when a function is critical, refer to the Council Risk Management Framework.

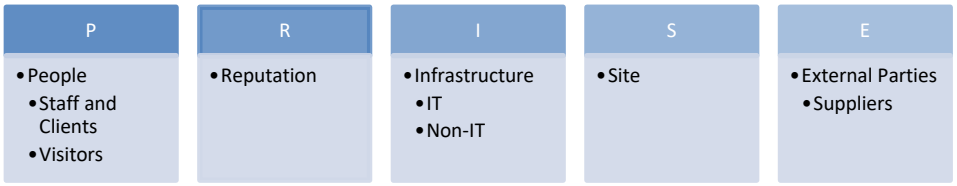
Criticality	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5 not critical	Tier 6 not critical
MAO	Immediate (<4 hours)	Today (5-24 hours)	Tomorrow (1-3 days)	This Week (4-7 days)	Next Week (8-14 days)	Eventually (>14 days)

2.3 **Business Continuity Plans**

The Council will develop, implement and maintain business continuity plans (BCPs) in accordance with this policy, which aim to minimise the disruption to business operations in the event of a disruption and restore operations to normal levels as soon as possible after a disruption.

BCPs are approved by the Senior Leadership Team and must be reviewed and tested every two years. Alwyndor BCPs must be provided to the Alwyndor Management Committee for noting after each review.

Plans will follow an event neutral style (PRISE) – focussing on impact of outages rather than the event itself:



2.4 **Crisis Management**

Council will develop a Crisis Management Plan (CMP) to assist with strategic incident management command and control in response to a critical incident. Alwyndor will have a separate CMP.

The CMPs are approved by the Senior Leadership Team and must be reviewed and tested every two years.

The Crisis Management Team established under the CMP will provide advice to the Senior Leadership Team who will retain operational decision-making.

Crisis management decisions must give due regard to State Emergency directives, procedures and any relevant advice from the Local Government Functional Support Group.

2.5 **Suppliers and Service Providers**

All third-party suppliers providing critical business activities must provide evidence of the existence, updating, testing, outcome of testing, and security of the appropriate BCM plans for the critical business activities including details of the testing and their results. Where requested, these must be made available to the Council.

2.6 Training and Awareness

All staff with allocated BCM responsibilities within business continuity plans must be involved in the biennial reviews to enable them to understand their obligations and responsibilities.

3. REFERENCES

3.1 Legislation

- *Civil Liability Act 1936*
- *Emergency Management Act 2004*
- *Local Government Act 1999*
- *South Australian Public Health Act 2011*
- *Work Health and Safety Act 2012*

3.2 Other References

- AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines
- Audit Committee Terms of Reference
- Better Practice Model – Internal Financial Controls 2012 SALGFMG
- Risk Management Policy and Framework
- Emergency Operations Manual
- WHS Emergency Management Policy
- Workplace Emergency and Evacuation Plans
- ICT Disaster Recovery Plan