Business Continuity and Disaster Recovery Framework and Policy

Version: 2.0

July 2017
Document control

Prepared for: Chief Minister, Treasury and Economic Development Directorate

Document Owner: Senior Manager Audit and Risk

File Name: CMTEDD Business Continuity and Disaster Recovery Framework and Policy

Version: 2.0

Status: Final

Revision

This Business Continuity and Disaster Recovery Framework and Policy must be reviewed and updated every two years (or more frequently following major change to business operations and/or priorities) as a part of Chief Minister, Treasury and Economic Development Directorate business planning process.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Final</td>
<td>July 2016</td>
<td>Senior Manager Audit and Risk.</td>
</tr>
<tr>
<td>2.0</td>
<td>Final, changes are not material. Altered structure following administrative arrangements.</td>
<td>July 2017</td>
<td>Senior Manager Governance.</td>
</tr>
</tbody>
</table>

Review and authorisation

The Business Continuity and Disaster Recovery Framework and Policy are to be reviewed and endorsed by the Director-General, Chief Minister, Treasury and Economic Development Directorate.

13 July 2016

David Nicol
A/g Director-General
Chief Minister, Treasury and Economic Development Directorate
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Purpose</td>
<td>4</td>
</tr>
<tr>
<td>Application</td>
<td>4</td>
</tr>
<tr>
<td>Business Continuity Policy Statement</td>
<td>5</td>
</tr>
<tr>
<td>What is Business Continuity Management?</td>
<td>6</td>
</tr>
<tr>
<td>Understanding the Business Continuity Management Lifecycle</td>
<td>6</td>
</tr>
<tr>
<td>Applying Risk Management Principles into Business Continuity Planning</td>
<td>7</td>
</tr>
<tr>
<td>CMTEDD Roles and Responsibilities for Business Continuity Management</td>
<td>7</td>
</tr>
<tr>
<td>Business Continuity Planning within CMTEDD</td>
<td>9</td>
</tr>
<tr>
<td>Business Continuity Plans</td>
<td>9</td>
</tr>
<tr>
<td>CMTEDD Business Continuity Plan</td>
<td>9</td>
</tr>
<tr>
<td>CMTEDD Business Continuity Structure</td>
<td>9</td>
</tr>
<tr>
<td>Understanding the need for a Business Continuity Plan</td>
<td>10</td>
</tr>
<tr>
<td>Business Impact Analysis (BIA)</td>
<td>11</td>
</tr>
<tr>
<td>BIA Conclusion</td>
<td>12</td>
</tr>
<tr>
<td>Business Continuity Plan Structure</td>
<td>12</td>
</tr>
<tr>
<td>Distribution of and access to the BCP</td>
<td>12</td>
</tr>
<tr>
<td>Testing and Maintenance</td>
<td>13</td>
</tr>
<tr>
<td>Unplanned Outages</td>
<td>13</td>
</tr>
<tr>
<td>Monitoring and review</td>
<td>14</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>14</td>
</tr>
<tr>
<td>What is disaster recovery?</td>
<td>14</td>
</tr>
<tr>
<td>Whole of Government Disaster Recovery Plan</td>
<td>14</td>
</tr>
<tr>
<td>DR Planning and Maintenance Activities</td>
<td>14</td>
</tr>
<tr>
<td>ICT System Owners Responsibilities</td>
<td>14</td>
</tr>
<tr>
<td>Business Continuity Management Maturity</td>
<td>15</td>
</tr>
</tbody>
</table>
Introduction

Purpose

This Business Continuity Framework and Policy Statement detail the Business Continuity Planning process for Chief Minister, Treasury and Economic Development Directorate (CMTEDD). The need for developing and maintaining CMTEDD’s Strategic, Stream and Divisional level business continuity plans (BCP’s) arises from CMTEDD’s commitment to sound risk management and corporate governance practices.

The Framework and Policy Statement outline the Directorates commitment to undertaking the delivery of critical services to our stakeholders, including our staff, Ministers and the Community following a Business Interruption Event (BIE) and aims to build resilience and capability across all areas of the Directorate.

CMTEDD acknowledges that business interruption-related risks may be infrequent, however may have severe consequences on the effective delivery of critical services. Business interruption-related events generally, are not able to be resolved by routine management. They include physical and non-physical events such as natural disasters, pandemics, significant loss of infrastructure (including ICT infrastructure), financial crises, and incidents that threaten our safety, reputation and viability. An effective Framework equips us to:

- ensure services that are critical to our objectives continue despite the occurrence of a potentially business interruption
- stabilise the effects of a business interruption event and return to normal operations and a full recovery as quickly as possible
- capitalise on opportunities created by the business interruption event

This adaptive capability aims to build high level resilience within the organisation, and

- minimise financial effects and effects on service delivery targets
- improve understanding of functions and opportunities for improvement
- enhance stakeholder confidence
- protect corporate assets and reputation

The Directorate’s Business Continuity Plans (BCPs) have been developed by drawing upon a range of contemporary public and private sector methodologies including:

- Australian National Audit Office (ANAO) Business Continuity Management – Guide to Effective Control
- ANAO Business Continuity Management – Workbook
- AS/NZS 5050:2010 Business Continuity – Managing disruption related risk

Application

The Business Continuity Framework and Policy Statement apply to all employees and contractors engaged under the CMTEDD Portfolio, with the exception of Statutory Authorities unless otherwise agreed.
Business Continuity Policy Statement

Business Continuity Management is a core component of good governance and supports the CMTEDD Risk Management Framework. Business Continuity Management focuses on our capacity to achieve our objectives where a business interruption risk has been realised.

Business Continuity Planning activities must be undertaken utilising the fundamental principles and guidance detailed in the CMTEDD Risk Management Framework and Policy, and Risk Management Plan.

CMTEDD’s first priority in the case of a business interruption event is the immediate and ongoing safety of employees, contractors and visitors/patrons of CMTEDD premises. CMTEDD and whole of Government Emergency Management arrangements help to be prepared for, and respond to emergency situations and are separate to business continuity activities.

Emergency Management activities are to take precedence over the activation of any of CMTEDDs Business Continuity or Disaster Recovery Plans.

Following a business interruption event, CMTEDD will aim to ensure that critical services are operating or resumed as quickly as possible, and that returning to business as usual is undertaken as efficiently as possible.

CMTEDD will reflect on and review our experiences of business interruption events and apply lessons learnt into our business continuity management planning activities to minimise (where possible) their consequence and likelihood in the future.
What is Business Continuity Management?
As defined by the ANAO Business Continuity Better Practice Guide 2009

“Business Continuity Management (BCM) is the development, implementation and maintenance of policies, strategies and programs to assist an entity manage a business disruption event, as well as build entity resilience. It is the capability that assists in preventing, preparing for, responding to, managing and recovering from the impacts of a business disruption event.”

Understanding the Business Continuity Management Lifecycle
The business continuity management lifecycle can be broken down into six distinct stages as outlined in the below table. As with the risk management process, it should be treated as a cyclical process requiring open and transparent communication with stakeholders and continual monitoring and review processes in place for each stage to produce value add outcomes.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Key Outcomes</th>
<th>Process Category</th>
<th>Process Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduce</td>
<td>Reduce the likelihood or consequence of interruptions occurring</td>
<td>This is part of ongoing risk management</td>
<td>Business Resilience Plans or work around procedures</td>
</tr>
<tr>
<td></td>
<td>Select and implement backup strategies and agreements</td>
<td>This should be treated as business as usual</td>
<td>Risk Assessments</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Risk Treatment Action Plans</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ICT Systems Security Plans</td>
</tr>
<tr>
<td>Respond</td>
<td>Protect life, safety and assets</td>
<td>This is the role of emergency procedures</td>
<td>Emergency Management Plans</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ICT Incident Management Plans</td>
</tr>
<tr>
<td>Recover</td>
<td>Establish temporary operations for time-critical business functions, moving to alternative sites, setting up for alternative processing</td>
<td>This is Business Continuity</td>
<td>Business Continuity Plan</td>
</tr>
<tr>
<td>Resume</td>
<td>Deliver time-critical services using alternative arrangements</td>
<td>This is Business Continuity</td>
<td>Business Continuity Plan</td>
</tr>
<tr>
<td>Restore</td>
<td>Rebuild damaged infrastructure</td>
<td>This is (operational) disaster recovery</td>
<td>Restoring operations may be linked to a strategic planning process indicative of the type of BIE</td>
</tr>
<tr>
<td></td>
<td>Deliver non-critical services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Return</td>
<td>Return to normal operations</td>
<td>Business as Usual</td>
<td>Apply lessons learnt from BIE and review/update any plans processes as required</td>
</tr>
</tbody>
</table>
Applying Risk Management Principles into Business Continuity Planning

As with the CMTEDD Risk Management Framework and Policy Statement the 11 principles of risk management defined by AS/NZ ISO 31000:2009 are to be adopted and fostered by the Senior Executive in the development of business continuity planning processes:

1. Creating and protecting value
2. An integral part of all organisational processes
3. Part of decision-making
4. Explicitly addressing uncertainty
5. Systematic, structured and timely
6. Based on the best available information
7. Tailored
8. Human and cultural factors
9. Transparent and inclusive
10. Dynamic, iterative and responsive to change
11. Continual improvement of the organisation

CMTEDD Roles and Responsibilities for Business Continuity Management

Risk governance mechanisms embed into CMTEDD’s organisational culture aims to ensure transparency, accountability and the appropriate level of authority is aligned with the end to end management of business continuity planning within the directorate.

Roles and accountabilities within CMTEDD are outlined as follows:

Executive Management Group

- Endorse the CMTEDD Business Continuity Framework and Policy Statement
- Endorse business continuity plans applicable to their area of delegation and authority
- Undertake, delegate and approve business continuity roles as appropriate
- Continual development of knowledge and skills in business continuity

Deputy Directors-General, Executive Directors, Directors

- Development, ownership, and maintenance of business continuity plans, in line with the Business Continuity Framework and Policy
- Incorporating risk management principles into business continuity planning operations
- Undertake, delegate and approve business continuity roles as appropriate
- Ensuring staff and contractors understand and fulfil their business continuity roles
- Reporting and providing advice to the Executive Management Group business continuity matters including escalating issues when appropriate
- Continual development of knowledge and skills in business continuity
Senior Managers and Team Leaders

- Undertake, understand and build capability with business continuity roles as appropriate
- Encourage staff to develop knowledge of business continuity processes, and actively participate business continuity processes
- Development, ownership, and maintenance of operational risks indicative of their respective areas of responsibility, including, identifying, treating risks that may impact on business continuity objectives
- Regular review of the adequacy of internal controls to ensure the intended level of treatment is maintained and aligns with business continuity objectives
- Reporting and providing advice to the Executive on business continuity related matters including escalating issues when appropriate

Staff and Contractors

- Develop an understanding of roles and responsibilities in relation to business continuity planning processes
- Actively supporting and contributing to business continuity planning processes

CMTEDD Corporate

- Development and maintenance of CMTEDD Business Continuity Framework and Policy
- Coordinate the development, review and testing of Tier 1 and Tier 2 BCP’s
- Development of BCP test schedule
- Provide advice to support, where required for CMTEDD business continuity planning activities of Tier 3 BCP’s.
- Reporting business continuity management activities to the CMTEDD Audit and Risk Committee

Internal Audit Providers

- In consultation with the CMTEDD Internal Audit Manager, initiate independent reviews in relation business continuity processes.
Business Continuity Planning within CMTEDDD

Business continuity management within the Directorate involves the following key steps:

- Undertaking strategic and operational risk assessments, and applying treatments to minimise the consequence and or likelihood of disruptions to business activities
- Conducting a business impact analysis, including the identification of key resource requirements
- Development of response strategies; and
- Development of Business Continuity, Disaster Recovery or Business Resilience Plans/ workarounds

Business Continuity Plans (BCP’S) are categorised into three distinct levels of management;

- **Tier 1** – BCP is fully maintained and reviewed by the Audit and Risk team in consultation with the Continuity Management Team and tested at least every 12 months
- **Tier 2** – BCP is reviewed and tested by the Audit and Risk team within 12 to 24 months
- **Tier 3** – Division/Business Unit is responsible for updating and testing of the BCP

The level of management and maintenance of BCP’S within the Directorate is tailored in accordance with the overall impact, loss, disruption or risk to critical functions.

**Business Continuity Plans**

BCP’s identify, analyse and record potential business impacts, recovery priorities and management strategies. They also describe the business continuity management structure, staff roles and responsibilities, and actions that are to be implemented after a major incident.

It is important to note that the BCPs are to act as a guide only; sound practical judgement should be applied to any plan to suit a particular situation.

**CMTEDDD Business Continuity Plan**

The CMTEDDD BCP is a top level directional plan for the Directorate, and will operate in the event that one or more CMTEDDD BCP’s are activated, or in the event that another ACT Government Directorate requires assistance to continue critical operations following a business interruption event (BIE).

The CMTEDDD Plan establishes a centralised Control Centre and provides support to each of the activated plans and provides oversight and coordination of Communications and Media activities, ICT, HR, Finance and Corporate (Facilities).

**CMTEDDD Business Continuity Structure**

The CMTEDDD business continuity structure has been developed to address the dual role of the Head of Service (HOS) and Director-General CMTEDDD. The structure enables the delegate to exercise powers in the capacity of either role and determine actions when dealing with an internal, external or whole of government business interruption event (BIE).
The Streams, Divisions and Business Units currently managed by CMTEDD Corporate each have a Business Continuity Plan (BCP) to support their business operations as depicted in the below BCP structure.

**Figure 1: CMTEDD Business Continuity Structure**

Understanding the need for a Business Continuity Plan

Undertaking a business impact analysis (BIA) will determine the level of continuity planning required by the area undertaking the BIA and provide a platform for an appropriate response strategy to manage disruption related risk. It is important to note that a fully integrated BCP may not always be the best solution for all areas considering developing a BCP, especially where identified critical business activities or processes have a negligible effect on the ability of CMTEDD or the ACT Government to meet its key objective.
Business Impact Analysis (BIA)

Conducting a Business Impact Analysis is the process of identifying critical business activities or processes which must be performed by the directorate to enable the ACT Government to meet its most important objectives. These should be vital activities, processes or systems that without, the ACT Government will either not survive, or will lose the capability to effectively achieve its objectives.

Identifying business critical activities, and or processes essential to achieving organisational and government key objectives is the first step in conducting a BIA. Defining business processes including interdependent processes critical to achieving the objectives is also a key component of articulating the activities.

A typical business impact analysis should also define the following categories:

- **Minimum resource requirements** for each process including people, facilities, information and communications technology, vital records, and dependencies or interdependencies. Consideration must also be given to alternate workaround procedures in the absence of any identified resource requirements;
- **Maximum Tolerable Period of Disruption (MTPD)** that being, the maximum period of time that the organisation can tolerate the interruption to a critical business process, before the achievement of objectives is adversely affected;
- **Recovery Time Objective (RTO)** The target time set for the recovery of an activity, product, service, or critical business process after a business interruption event; or Recovery of an IT system or application after a business interruption event;
- **Recovery point objective (RPO)** is a measure of data loss. It is the point in time (before the business disruption) to which electronic data must be recovered after a business interruption event. All data between that point and the time of the disaster is lost. The larger the acceptable RPO, the more data loss each critical application can tolerate before it becomes a problem for the business critical process; and
- **An Impact rating** is to be applied to the critical activity. The rating is to be based on the absence of undertaking the critical process or activity and the impact it has on the delivery of the Directorate’s functions. Consideration should be given to what the impact may be on internal and external stakeholders, including; other directorates, the ACT government, businesses and the community.

The level of impact of business disruption is assessed using the following scale:

<table>
<thead>
<tr>
<th>Level of Impact</th>
<th>Consequence of impact</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extreme</td>
<td>Threatens political and business viability</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>Significant impact on business drivers</td>
<td>4</td>
</tr>
<tr>
<td>Moderate</td>
<td>Major impact on short term business operating</td>
<td>3</td>
</tr>
<tr>
<td>Low</td>
<td>Inconvenient but no real ongoing business impact</td>
<td>2</td>
</tr>
<tr>
<td>Negligible</td>
<td>Reconsider the inclusion of this as a critical resource</td>
<td>1</td>
</tr>
</tbody>
</table>

Each of the above BIA categories may need to be defined or broken down multiple times depending on the context of the area undertaking the BIA. Examples may include time critical activities such as delivery of the
ACTPS Pay run or processes with legislative deadlines. Alternately, some categories may not necessarily apply to each critical business process or activity. A BIA needs to be tailored to suit each area undertaking the BIA.

**BIA Conclusion**
Scrutiny of the finalised BIA should establish the type of ongoing business continuity planning process to be undertaken by the relevant area. Determining the level of BCP required should be done in consultation with Executives potentially involved in the continuity reporting hierarchy, and in consultation with the CMTEDD Business Continuity Manager.

**Business Continuity Plan Structure**
Each CMTEDD Stream, Division and Business Unit BCP follows the same systematic approach to the overall development and structure of each individual BCP document, but are tailored to meet the context of the specific recovery strategies. The minimal BCP structure requirements are detailed as follows:

**Introduction** – Details the scope and context of the business area and should clearly reflect its key objectives and or priorities

**Activation** – Provides guidance and suggested procedures when considering activating the BCP

**Crisis Management Team (CMT)** – details the roles, responsibilities and suggested actions of the business area

**Recovery Arrangements** – details alternate arrangements for the establishment of the CMT and alternate processing facilities

**Contact Lists** – Identify key contacts/stakeholders, both internal and external

**Business Impact Analysis** – details critical business activities, processes and recourses required for continuity of critical activities

**Information systems restoration priorities** – identifies critical ICT systems and recovery time objectives

**Vital records identification** – Identifies vital records imperative to undertaking critical business activities

**Templates and checklists** – A suit of documents for guidance and recording activities and decisions whilst the BCP is activated

**Distribution of and access to the BCP**
BCP’s should be made accessible to all staff potentially involved the continuity or recovery processes. BCP owner’s should consider access to hard copies; encrypted USB’s and shared drives for ease of access in any potential situation. All officers with identified roles in the BCP must be contactable into the event of a BIE and all contact numbers should be kept up to date and accessible. Audit and Risk make available all BCP’s vial the Executive Portal.
Testing and Maintenance
CMTEDD Audit and Risk maintain a testing schedule and facilitate the testing of Tier 1 and Tier 2 Business Continuity Plans in line with the Audit Office recommendations. The plans are tested in a number of ways, test types include the following:

Desktop review: is normally conducted as one of the first plan ‘tests’, it involves a physical examination and review of the plan documentation. A Desktop review aims to ensure that:

- the plan document is complete and relevant to the expressed business needs (operational and strategic)
- the relevance and currency of the risk assessment, business impact assessment and continuity plan are tested
- inconsistencies in logical flow, resources allocations or conflict between individual plans are recognised
- all required data, supplies and/or other hardcopy documents are actually backed up and correctly stored off-site

Desktop scenario test: Involves a desktop walkthrough of the plan(s), with discussion guided by the use of one or more potential scenarios. These tests will ensure the BCP procedures are adequate. Such tests require the development of a disaster scenario which leads the relevant CMTs through a mock recovery.

The activities are based around a series of questions and answers relating to the deployment of the plans in response to changing issues in the scenarios. A structured walk-through test is conducted as follows:

- all relevant team leaders are given a scenario
- each team leader works through his/her recovery and restoration plans, paying particular attention to any interaction(s) with other teams
- issues identified are to be noted by the Recovery Co-ordinator (and the necessary remedial action developed and BCP updated accordingly)

Notification and call-out communications test: Activities are based around the verification of the accuracy, currency and quality of notification and call-out lists, call out trees (who you have to call) and deputised positions.

Live scenario tests: Can be conducted as a limited activation (narrow/specic scenario and/or targeted areas of the organisation) up to a full scale activation of all continuity arrangements for the organisation.

Business recovery tests: Involves the closing down or removal of access to infrastructure or resources and test the capability of recovery measures.

Unplanned Outages
Business units should record all unplanned outages or disruptions affecting the service delivery to their individual operations. Examples of outages include the loss of power or evacuation at a territory venue or shopfront, or a disruption or outage to a government or business critical ICT system.
Monitoring and review
Each BCP should be monitored and reviewed regularly. Review processes and updates should be applied in the following circumstances:

- after exercising the plan
- following a business interruption event
- when a change in business priorities occurs
- following a change to organisational structures and
- In line with statutory requirements

BCP Response Directors and Crisis Management Team Leaders have responsibility for maintaining up to date documentation. All Changes should be administered through the CMTEDD Business Continuity Manager.

Disaster Recovery

What is disaster recovery?
Disaster recovery is the mechanism for which IT systems, infrastructure and assets are recovered after an interruption in line with the Directorate’s priorities.

Whole of Government Disaster Recovery Plan
The ACT Government ICT Disaster Recovery Plan describes arrangements that Shared Services ICT will use to manage the recovery of, ACT Government critical systems, directorate business critical systems, ICT Assets and ICT Infrastructure which have been impacted by a major, unexpected and disruptive event. The DRP outlines the management structure, staff roles and responsibilities, and actions that are to be performed after a major incident to assist with the recovery of ICT infrastructure and systems.

DR Planning and Maintenance Activities
Shared Services has responsibility for developing and maintaining the ACT Government ICT Disaster Recovery Plan in conjunction with all directorates, agencies and community facilities utilising the act.gov network and ACT Government data centres.

ICT System Owners Responsibilities
ICT Systems owners must ensure they are aware of their systems restoration, backup and recovery procedures. Where applicable, manual workaround procedures should be up to date and accessible where system full High Availability (HA) is not an active treatment mechanism.

System owners must maintain up to date communications with Shared Services ICT representatives to ensure their systems are maintained with satisfactory disaster recovery process in place.
Business Continuity Management Maturity

In order to continually improve the adequacy of CMTEDD Business Continuity Plans as a risk treatment, CMTEDD Audit and Risk will audit selected BCP’s utilising a consistent, systematic assessment model developed from the Australian National Audit Office’s (ANAO) ‘Business Continuity Management: Building resilience in public sector entities’ and COBIT Maturity Model.

The assessment will be conducted through interviews along with a review of selected plans, policies and procedures. A detailed assessment model is provided in the CMTEDD BCP Testing Schedule.