Business Continuity Management

# Purpose

To ensure systems and processes are in place for the continuity of critical business functions in the event of a disruptive incident, in accordance with the requirement to manage material risk outlined in *Treasurer’s Instruction 825: Risk management and security*.

Business continuity management (BCM) at the Department of Health (department) is an important component of the Risk Management Framework and aligns with the requirements of *AS ISO 22301 Security and Resilience – Business Continuity Management System.*

# Applicability

This policy is applicable to Department of Health employees whether permanent, fixed term, contract or casual.

# Policy requirements

The department adopts an integrated risk-based approach to BCM and establishes plans to ensure continuity of its critical business functions. Planning and preparation activities and the process for incident response and recovery are outlined in the department’s BCM Framework.

## BCM Framework

The department will maintain an up-to-date, fit-for-purpose BCM Framework that provides assurance to the Director General (DG), Department Executive Committee (DEC), and the Risk and Audit Committee (RAC) that disruption-related risks are clearly identified and managed appropriately, with consideration to the Department’s risk appetite and objectives, and that business continuity can be maintained should a disruption occur.

Divisions are responsible for undertaking planning activities outlined in the BCM Framework, consisting of the following key components:

* risk identification and assessment
* business impact analysis
* business continuity planning
* regular testing and training.

This includes maintaining up-to-date business continuity plans (BCPs) which define the priorities and processes to respond, recover, restore and resume the division’s critical business functions (CBF) to a pre-defined level of operation.

The department maintains a defined incident notification and escalation process outlined in the BCM Framework. Critical events are escalated to the department’s business continuity team (BCT) which is responsible for coordination of a department-wide response and recovery from critical events. A representative from each division will be appointed to the BCT.

## Roles and responsibilities

### Director General

The DG is ultimately accountable for the continuity of the department’s business operations.

### Department Executive Committee

The DEC is responsible for overseeing the continuity of the department’s business operations and for:

* maintaining oversight of disruptive risks with the potential to affect the department’s operations
* approving the content of, and any subsequent amendments to the BCM Policy and BCM Framework.

### Risk and Audit Committee

The RAC monitors the effectiveness of the BCM Framework ensuring alignment with the *AS ISO 23001*. The RAC’s functions are outlined in the Department of Health Risk and Audit Committee: Terms of Reference.

### Deputy Director General

As the BCT Lead, the DDG is responsible for the management and coordination of the department’s recovery efforts from a critical incident.

### Assistant Directors General

Approve updates to divisional BCPs; support regular updating, testing and exercising of divisional BCPs.

### Department senior executives and management

Department executives and management are responsible for the identification, ownership, and management of their disruption related risk(s). Risks with the potential to disrupt the business activities within their areas of responsibility and authority are to inform their BCP.

### Employees

Departmental employees have a role in managing risk and ensuring that disruptions to the department’s business operations is optimally managed. This role requires their participation in the BCM process to identify disruption risk(s) and mitigating controls and the development of business workarounds.

### Risk and Audit Unit

The Department’s Risk and Audit Unit is responsible for:

* collaborating with risk owners to ensure that disruption risks are identified, recorded, and managed in the enterprise risk management system
* developing and maintaining this policy and its supporting documents
* assisting in the development and periodic review of business impact analyses
* ensuring that all BCPs, BCT callout tree and action cards are available and up-to-date should a BCP be activated
* providing support, guidance and training to the employees in BCM processes
* reporting to the DEC and RAC on the status of the department’s BCM.

# Compliance monitoring

The effectiveness of BCM will be monitored and tested at least every 2 years. Compliance with this policy will be measured by:

* the use of risk information that supports the ongoing review and update of divisional BCPs
* monitoring and testing of BCM arrangements
* periodic auditing of the department’s BCM practices
* feedback from the DEC and RAC.

# Related documents

The following documents are mandatory pursuant to this policy:

* Department of Health: Business Continuity Management Framework.

# Supporting information

The following standards inform this policy:

* AS ISO 22301 *Security and resilience – Business continuity management systems – Requirements*
* AS ISO 31000: 2018 *Risk management – Guidelines.*

# Definitions

The following definitions are relevant to this policy.

|  |  |
| --- | --- |
| Term | Description |
| Business Continuity Management  | A management process that helps manage the risk to the smooth running of an organisation or delivery of a service, ensuring that it can operate to the extent required in the event of a disruption. |
| Business Continuity Plan | Documented procedures that guide the department to respond, recover, resume, and restore to a predefined level of operation following a disruption.  |
| Business Continuity Management Team | Designated individuals with responsibility for developing, execution, rehearsals, and the maintenance of the BCP. |
| Business Function | A description of the work that is performed to accomplish a specific business requirement.  |
| Business Impact Assessment | A method of assessing the impacts of an event that might result from an incident and the levels of resources and time required for recovery. |
| Critical Business Function | The critical operational and/or business support functions that cannot be interrupted or unavailable. At the department a CBF is a function with a Maximum Tolerable Period of Disruption (MTPD) of 3 days or less as determined in the business impact analysis. |
| Disruption | An event that interrupts normal business, function, operations, or processes, whether anticipated or unanticipated.  |
| Escalation | The process by which event-related information is communicated upwards through the department’s established levels of delegated authority. |
| Maximum Tolerable Period of Disruption  | MTPD refers to the time within which a business activity or service must be resumed following a disruption. It is measured from the time a disruption occurs to the time when the activity or service becomes operational again.  |

# Approval and review

This mandatory policy is approved in accordance with the Policy governance procedure and will be reviewed as required to determine effectiveness, relevance, and currency. At a minimum it will be reviewed every 3 years.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version**  | **Effective from** | **Effective to** | **Amendment(s)** | **Authorisation** |
| 1.0 |  |  | Original version | Deputy Director General |
|  |  |  |  |  |

The review table indicates previous versions of the mandatory policy and any significant changes.

The owner of this policy is the **Director, Corporate Services, Office of the Deputy Director General.**

Enquiries relating to this policy may be directed to the Manager, Risk and Audit doh.riskandaudit@health.wa.gov.au

**This document can be made available in alternative formats on request for a person with a disability.**

© Department of Health 2022

Copyright to this material is vested in the State of Western Australia unless otherwise indicated. Apart from any fair dealing for the purposes of private study, research, criticism, or review, as permitted under the provisions of the Copyright Act 1968, no part may be reproduced or re-used for any purposes whatsoever without written permission of the State of Western Australia.