1. Statement

Business continuity management (BCM) practices and business continuity plans (BCP) effectively support preparedness, prevention, response and recovery from a disruptive event, and continuity of key functions. BCM forms a critical part of managing disruption risks and ensuring an effective system for risk management is in place.

2. Scope

This standard applies to all divisions and business units within the Department of Health.

2.1 Relationship to crisis management arrangements

Crisis management is the response to a situation that is beyond the capacity of business as usual management structures, resources and processes. This may include disruption of key functions. The department’s crisis management arrangements are outlined in the department’s Crisis and Continuity Plan (CCP).

2.2 Relationship to State health disaster management arrangements

Queensland Health has responsibilities under the Queensland State Disaster Management Plan to provide health-related functions and services, and to participate in multi-agency disaster management groups at local, district and state levels. Refer to the Queensland Health Disaster and Emergency Incident Plan for further information about disaster and emergency incident plans and arrangements. The resource requirements or impacts of disasters or emergency incidents may require BCPs to be activated in parallel with disaster and emergency plans. This will primarily be to manage surges in staffing requirements to ensure continuity of health services to the community, or to maintain critical business functions in cases of impact to facilities or systems.

3. Requirements

This implementation standard identifies the minimum mandatory requirements for the governance and management of business continuity arrangements to manage disruption risks.

3.1 Overview

Continuity arrangements will identify processes, controls and resources needed to ensure critical business functions continue to be delivered in the event of a disruption.

The department’s Business Continuity Management Guideline provides guidance, tools and templates for BCP and function owners to achieve these requirements.

3.2 Responsibilities

3.2.1 The Director-General establishes and maintains appropriate systems of internal control and risk management in accordance with the Public Sector Ethics Act 1994, Financial Accountability Act 2009 and Financial and Performance Management Standard 2009.

3.2.2 Deputy directors-general/chief executives/commissioners of accountability areas shall:

- maintain and oversee their business continuity arrangements and a divisional/business unit BCP
• determine if additional/subordinate BCPs are required for business units, physical location or specific functions/processes
• ensure capability to conduct business continuity management is maintained for their accountability area
• communicate the importance of effective business continuity management and ensure staff are aware of their roles and responsibilities to ensure effective response to disruptive events.

3.2.3 The Chief Risk Officer shall:
• develop and maintain an effective BCM system and support its implementation
• ensure annual reporting on BCM arrangements in line with this standard and seasonal preparedness activities
• provide advice in relation to business continuity management
• maintain, support and distribute the department’s CCP.

3.2.4 Owners of BCPs shall:
• coordinate the analysis, documentation and communication of disruption risk and continuity arrangements across functions, application and data
• maintain the BCP in a current state and distribute relevant BCP information to appropriate stakeholders
• ensure resources identified in BCPs are available or coordinate alternative arrangements
• test and exercise continuity arrangements at appropriate intervals with key stakeholders (internal and external)
• record and review lessons from tests and disruptive events
• notify relevant stakeholders as per CCP and BCP requirements when the BCP is activated or deactivated
• ensure that BCPs are linked to supporting arrangements, agreements, and plans including the CCP, state health disaster management arrangements and ICT disaster recovery planning
• ensure that BCPs are based on a business impact analysis (BIA) and identified disruption risks
• ensure that BCPs are reviewed at least annually, or more frequently if needed based on the level of disruption risk and any changes in organisational context
• where applicable, document:
  − the BCP owner
  − criteria for BCP activation and deactivation
  − time critical business functions
  − response and recovery strategies to mitigate the effects of disruptions and return to business as usual including any resource requirements
  − contact details for relevant personnel and stakeholders
  − roles and responsibilities for BCP participants
  − communication strategies to keep staff, supplies and stakeholders informed
  − internal and external interdependencies including critical information systems
  − agreed and supported actions by upstream providers and downstream customers where relevant.
3.2.5 Positions responsible for business functions where relevant, or required to support BCP owner responsibilities, are to:

- develop and maintain business continuity arrangements for the function
- contribute to the relevant BCP
- provide expert advice to support business impact analysis.

3.2.6 ICT service providers or positions responsible for technologies required to support an application are required to:

- provide information pertaining to business function continuity arrangements to function owners including system capability, ICT Disaster Recovery (ICTDR) planning measures and recovery objectives
- ensure ICT defined recovery times, priorities and activities are discussed, understood and agreed with business areas
- include recovery point objectives as a service level agreement criterion for negotiation and agreement
- prioritise ICT disaster recovery activities for all critical business functions and associated ICT assets
- participate in testing and exercises for continuity arrangements related to ICT assets
- contribute to business continuity arrangements and BCPs developed by BCP owners.

3.2.7 Contract managers, service managers and project managers when involved in work that affects or supports a critical business function are required to:

- comply with and participate in strategies for preparedness, prevention, response and recovery including ensuring appropriate monitoring and governance
- proactively communicate risks with relevance to critical business functions to their responsible executive and/or governing board
- consider any necessary provisions to support business continuity and/or ICT disaster recovery in contracts and third party agreements.

3.2.8 All staff are required to:

- be aware of the department’s business continuity arrangements and expectations
- comply with and participate in preparedness, prevention, response and recovery strategies to ensure business continuity of critical business functions.

4. Legislation

- Public Sector Ethics Act 1994
- Financial Accountability Act 2009
- Financial and Performance Management Standard 2009

5. Supporting documents

- Risk Management Policy (QH-POL-070)
- WHS Risk Management Implementation Standard (QH-IMP-401-3)
- Queensland Health Disaster and Emergency Incident Plan (QHDISPLAN)
- Business Continuity Management Guideline
- Crisis and Continuity Plan
- AS/NZS 5050:2010 Business continuity – Managing disruption related risk
- ISO 22301:2012 Societal security – Business continuity management systems
## 6. Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business continuity</td>
<td>The uninterrupted availability of essential business functions.</td>
</tr>
<tr>
<td>Business continuity management (BCM)</td>
<td>A holistic management process that allows an organisation to identify potential threats and impacts to business operations, if realised, might cause, and which provides a framework for building organisational resilience with the capability to effectively manage disruption related risks against critical business functions.</td>
</tr>
<tr>
<td>Business continuity plan (BCP)</td>
<td>Documented procedures that provide guidance on how to prepare, prevent, respond and recover from a disruptive event. This includes business activities associated with maintaining availability of people, assets and property vital for the continuity of critical business functions.</td>
</tr>
<tr>
<td>Crisis</td>
<td>A situation that is beyond the capacity of normal management structures, resources and processes to deal with effectively.</td>
</tr>
<tr>
<td>Critical business functions / Critical processes</td>
<td>A business function, or part of a function (process) without which the organisation will suffer significant impact. If a critical business function or process is non-operational, the organisation could suffer serious legal, financial or reputational damage. Refer to the Risk Consequence Table for more detailed analysis.</td>
</tr>
<tr>
<td>Disruptive event</td>
<td>An event that threatens to disrupt critical business functions</td>
</tr>
<tr>
<td>Information and communication technology disaster recovery (ICTDR)</td>
<td>The process, policies and procedures related to preparing for recovery or continuation of technology infrastructure, systems and applications which are vital to an organisation after a disaster or outage. Note: ICTDR focuses on the information, communication or technology systems that support business functions, as opposed to Business Continuity which involves planning for keeping all aspects of a business functioning in the midst of disruptive events. ICTDR enables good business continuity practice.</td>
</tr>
<tr>
<td>ICT service provider</td>
<td>A position designated with responsibility for the technologies required to support the application including software technologies, hardware and network support. Technologies are involved with either essential infrastructure or general productivity software and hardware; an application is related to particular business processes.</td>
</tr>
<tr>
<td>BCP owner</td>
<td>The position that owns a BCP whether for a Division, business area, branch, unit or function.</td>
</tr>
</tbody>
</table>

### Version Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>15 June 2017</td>
<td>Implementation standard for business continuity management</td>
</tr>
</tbody>
</table>