SA Health

Disaster Resilience – Business Continuity Management Framework

Version 3.2 October 2019

Government of South Australia

SA Health

Document Control Information

Document Owner:	Disaster Preparedness and Resilience Branch (DPRB)
Title:	SA Health Disaster Resilience - Business Continuity Management Framework
Description:	Outlines the purpose, scope and governance for the Business Continuity Management (BCM) Framework, including the ongoing BCM monitoring program across the BCM lifecycle.
Subject:	Business Continuity Management; Disaster Resilience; Disaster Management
Document Location:	2019-01593
ISBN	978-1-76083-133-2
Next Review	July 2022

Version	Author	Comments	Approved	Date
1.0	Emergency Management Unit (EMU)	Original version	Portfolio Executive	June 2008
2.0	EMU	Complete re-write of the entire document	Portfolio Executive	June 2013
2.1	EMU	Updated milestones	Director, EMU	Dec 2014
3.0	EMU	Complete review and update of content, in light of Deloitte review 2017, and updates to standards and guidelines in 2018. Content inclusive of stakeholder feedback.	SAHDRC (Tier 1 Committee)	June 2019
3.1	DPRB	Minor update due to change of governance committee name to Department Executive Committee	Director, DPRB	Aug 2019
3.2	DPRB	Minor updates to assurance, BCP documentation, roles and responsibilities to bring in line with the updated Disaster Resilience Policy Directive.	SAHDRC (Tier 1 Committee)	Oct 2019

Contents

Document Control Information **2**

Background **4**

Introduction 4

Standards and guidelines 4

Glossary 4

Policy and Program **5**

Purpose 5

Context 5

Scope 7

Governance 7

Roles and responsibilities 8

Key Performance Indicators (KPIs) 9

Embedding **10**

Culture 10

Executive awareness and support 10

Organisational awareness 10

Analysis **11**

Risk 11

Business Impact Analysis (BIA) 12

Design **15**

BCP approach 15

Implementation **16**

Assess and activation 16

Response 16

Business Continuity Plan 18

BCP documentation 18

Control of documentation 20

Validation **20**

Training 20

Exercising 20

Post incident debrief 21

Monitoring and Review 21

Assurance 21

Introduction

The *SA Health Disaster Resilience - Business Continuity Management (BCM) Framework* (BCM Framework) provides a consistent set of principles for planning for, responding to and recovering from disaster and disruptive events, as well as an ongoing management program, to ensure a coordinated, integrated, whole of system approach across SA Health upon which it can measure its performance against and enhance disaster resilience. The implementation of the BCM Framework is a mandatory requirement for SA Health, as outlined in the *SA Health Disaster Resilience Policy Directive*.

Standards and guidelines

The BCM Framework is aligned with the BCI Good Practice Guidelines 2018 methodology and other contemporary industry standards and practices:

- AS/NZ ISO31000:2018 – Risk Management
- ISO22300:2018 – Security and resilience
- ISO22301:2017 – Societal security – Business continuity management systems
- ISO22313:2017 – Societal security – Business continuity management systems – Guidance
- ISO22317:2017 – Societal security – Business continuity management systems – Guidelines for business impact analysis (BIA)
- ISO22330:2018 – Security and resilience – Business continuity management systems – Guidelines for people aspects of business continuity
- AS3745:2010/Amdt1-2014 & Amdt2-2018 – Planning for emergencies in facilities
- AS4083:2010 – Planning for emergencies – Health care facilities
- BCI GPG:2018 – The Business Continuity Institute Good Practice Guidelines
- 2019 SA Health Disaster Resilience Policy Directive

Glossary

Please refer to the *SA Health Disaster Resilience Glossary* for all definitions used in this document.

Acronyms

The following acronyms are used in this document:

BAU	Business as usual
BC	Business continuity
BCM	Business continuity management
BCP	Business continuity plan
BDI	Business disruption incident
BIA	Business impact analysis
CBF	Critical business function
DRP	Disaster recovery plan
EM	Emergency management
IMT	Incident management team
ITSRP	Information technology service resumption plan (see also Disaster recovery plan)
MAO	Maximum acceptable outage
MBCO	Minimum business continuity objective
ROC Plan	Resource Outage Contingency Plan

Purpose

The BCM Framework is designed as a whole of system approach to provide consistent strategic direction to SA Health, and its key personnel, on the implementation of the BCM program.

The BCM Framework ensures that SA Health critical functions are able to continue delivering services following a business disruption incident, and aims to build high level resilience in all SA Health services and sites when facing major adverse events. It provides practical, flexible and scalable approach for BCM through the development and maintenance of robust, flexible and well exercised plans.

It is designed to build upon the current organisational capability through establishing a fit for purpose, strategic and operational program that:

- builds resilience and organisational capacity through the application of robust business continuity practices
- proactively improves SA Health's resilience against disruption to its ability to achieve its critical functions
- provides an exercised, demonstrated method of restoring SA Health's ability to supply its critical functions to an agreed level within an agreed time after business disruption incident
- focus on an 'all hazards approach' by addressing the consequences of the business disruption incident (ie effect on the availability of infrastructure, ICT, workforce) rather than on its cause
- delivers value to SA Health through linkage with business and clinical objectives
- delivers a proven capability to manage business disruption and protect SA Health's brand and reputation.

Context

SA Health is a high performing health organisation. High performing organisations are collaborative, robust, data and evidence-informed, transparent, partnership focussed, trusted, consistent and resilient during times of crisis.

The BCM Framework is also high performing, as content is evidence-informed and contemporary; roles and responsibilities are transparent; planning is robust; capability reflects a whole of system and all hazards approach; and content development has been collaborative in partnership with key stakeholders and it is applied consistently to all of SA Health.

The BCM Framework provides a structured approach to preparing for, responding to and managing significant business disruption incidents, that impact on normal operations. The incident management principles of this framework apply equally to business disruption incidents, regardless of their cause, as they do to any other emergency or adverse event.

In addition, the BCM Framework has a close relationship between Risk Management, Information Technology Service Resumption Management and Emergency Management, both within SA Health and corresponding government agencies in the emergency services sector. This aligns with the "comprehensive approach" principle which focuses on Prevention, Preparedness, Response and Recovery (PPRR) that underpins the Business Continuity and Emergency Management sectors.

Risk Management

The *SA Health Risk Management Policy Directive* states that risk can be defined as "the effect of uncertainty on objectives". Given that the goal of business continuity is to prevent, prepare for, respond to and recover from business disruption incidents, it is imperative that the business continuity planning process is incorporated as part of the enterprise-wide risk management framework.

Risk management seeks to identify and mitigate organisational risks through the identifying, analysing and evaluating a range of risks, and the development of treatments and controls. Often business disruption risks are identified in this process, so aligning business continuity activities with risk management activities (including the *SA Health Risk Management Framework*) ensures the identification, assessment and mitigation of business disruption related risks, as well as consistency of reporting and assurance activity across SA Health.

Information Technology Service Resumption Management

The *SA Health ICT Security Policy Directive* states that "Business units must maintain both a Business Continuity Plan and a Disaster Recovery Plan for the continuation of critical business services when information systems and assets are unavailable". There is a critical dependency on ICT systems for operational and support activities. Therefore, the process for developing and reviewing Business Continuity Plans within SA Health should be closely aligned with the process for developing, reviewing and testing Information Technology Service Resumption Plans (ITSRP) by Digital Health SA. These ITSRPs govern the procedures for the recovery of ICT systems both during and after a disaster that address key applications and infrastructure.

Aligning BCM with information technology service resumption management provides greater assurance that both operating and ICT systems recovery procedures meet the resumption requirements of SA Health entities for their critical functions and applications. This alignment is also consistent with the holistic approach to BCM and disaster recovery prescribed by ISO 22300:2018.

Emergency Management

The *State Emergency Management Plan* defines an emergency as "an event, actual or imminent, which endangers or threatens to endanger life, property or the environment, and which requires a significant and coordinated response".

Emergency management, like business continuity, seeks to strengthen organisation resilience, capability and capacity to prevent, prepare for, respond to and recover from emergency and/or disaster events through the development and maintenance of emergency management plans, training and exercising activities.

Aligning business continuity activities with emergency management activities (including the *SA Health Emergency Management Framework*) ensures that there are appropriate plans, training and structures in place to respond and recover from a business disruption, as well as consistency of process across SA Health.

Business Continuity Management

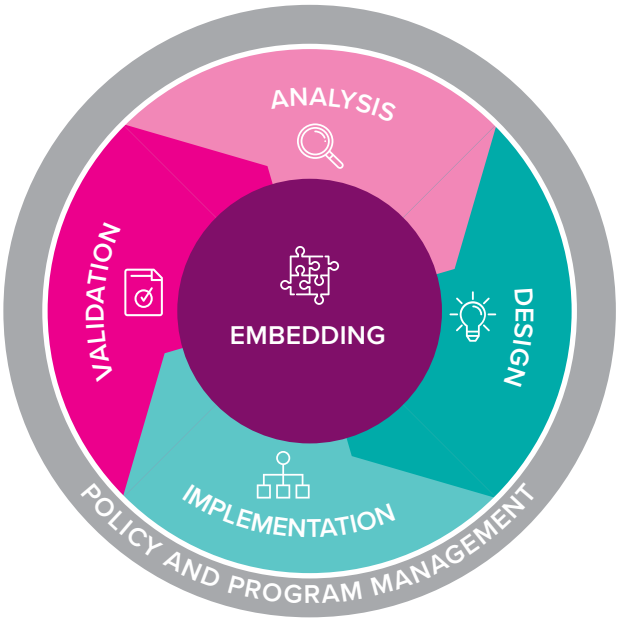
BCM is defined as a "holistic management process that identifies potential threats to an organisation and the impact those threats, if realised, can cause on business operations, and provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of key interested parties, reputation, brand and value-creating activities" (ISO 22300:2018 – Security and resilience – vocabulary)

BCM is a process that is engaged when normal business operations are unable to satisfactorily manage a business disruption incident and is required to modify / reduce its normal operations. This is often described as when a non-routine response is required to manage a business disruption incident, at which point the business continuity plan should be activated.

The development and maintenance of BCPs across SA Health ensures that there is strengthened organisational resilience and capability to prevent, prepare for, respond to and recover from business disruption.

Having a BCM program in place, which encompasses the above, ensures that business continuity and recovery requirements are both identified and addressed; resources are allocated; and processes and procedures are documented, trained and rehearsed. The program is most effective when policy and governance are in place to support it, implementation, compliance and effectiveness are managed, and all areas of the business have embedded BCM in their planning and operations.

Figure 1 – BCM Program (adapted from the 2019 *BCI: Good Practice Guide*)



An overview of the BCM program for SA Health is:

- Analysis – through the use of a Business Impact Analysis (BIA) tool identify and quantify any critical business impacts due to a business disruption event (loss or interruption of critical business activities). Activities at this stage include:
  - identifying all key business functions / processes
  - undertaking a business impact analysis (BIA) to identify all business processes and relevant maximum acceptable outage (MAO) periods for each function, along with resourcing (human and physical) requirements to operate during a business disruption incident
  - identification of business processes that are deemed critical and prioritise these as per their level of importance (Tier 1 & 2)
- Design – defines the operational requirements for business continuity and develops strategies that address the critical issues identified in analysis. Key discussions and activities are:
  - develop suitable workarounds or strategies to allow for a continuing provision of service, albeit in a reduced capacity
  - providing mechanisms for notification and alerting as well as escalation of business disruption incidents
  - providing a leadership and command / control structure to manage business disruption incidents
- Implementation – transform the strategies into capability through the development of plans (Strategic BCP, ROC Plan and Operational BCPs for critical functions) that details the resource capability and the key processes to follow to ensure the critical business services/functions continue to operate. This work includes:

- prepare and compile Business Continuity Plans (BCP) and Resource Outage Contingency (ROC) Plans
- communicate and socialise all BC arrangements to the organisation

> Validation – training and exercising the above plans with all staff to ensure familiarity, capability and currency. Key activities are:

- provision of education and training to staff, managers and executives in the area of business continuity
- undertaking of regular business disruption exercises and validation of BCPs as well as their relationship with emergency management arrangements
- regular review of business continuity documentation, including BCPs and their associated workarounds and strategies
- continuing to improve business continuity across SA Health.

Scope

The BCM Framework, and its implementation across SA Health, is a mandatory requirement for all SA Health, as outlined in the *SA Health Disaster Resilience Policy Directive*.

The scope of the BCM Framework is as follows:

> The Disaster Preparedness and Resilience Branch (DPRB), DHW is responsible for the BCM Framework and BCM program across all SA Health. The DPRB coordinates implementation of the BCM Framework and program across DHW, and provides facilitator and practitioner support to DHW areas. They also monitor, evaluate and report on the effectiveness of the BCM program through assurance activities. The DPRB also supports BCM Coordinators in Health Services and other areas specified below in their responsibilities under the BCM Framework.

> Health Services (LHNs, State-wide Services, SAAS) are responsible for the implementation of the BCM Framework and program, including sufficient resourcing of a BCM Coordinator. To achieve this, Health Services must develop and maintain effective plans and processes that are consistent with the BCM Framework, as well as effective review, training and exercising activities.

> Procurement and Supply Chain (PSCM) and Digital Health SA, due to their unique critical status (owing to their size, geographical spread and/or complexity), are also responsible for the implementation of the BCM Framework and sufficient resourcing for a BCM Coordinator support across their areas, including developing and maintaining effective plans and processes that are consistent with the BCM Framework, as well as training and exercising activities.

> The Infrastructure Programs Unit, DHW have a critical role in working with Deputy Chief Executives/Directors/Managers in identifying relevant sites and developing Resource Outage Contingency (ROC) Plans that meet organisational and business continuity requirements.

> All SA Health entities must ensure contracted Suppliers have effective business continuity arrangements in place (both within their own operations and supply chains, as well as any arrangements for supporting SA Health through the provision of goods or services during a disruption incident). These business continuity arrangements and requirements should be included in the terms and conditions of contracts (including service levels for supply disruption) as well as assessing the suitability of Supplier's business continuity program/documentation as part of any tendering process or as part of ongoing relationship management with the Supplier.

The scope of the BCM Framework does not cover emergency management arrangements. These can be found in the SA Health Emergency Management Framework.

Governance

Oversight, coordination and governance of the SA Health BCM Framework and Program will be modelled on the *SA Health Disaster Resilience Policy Directive* governance, and will comprise the following:

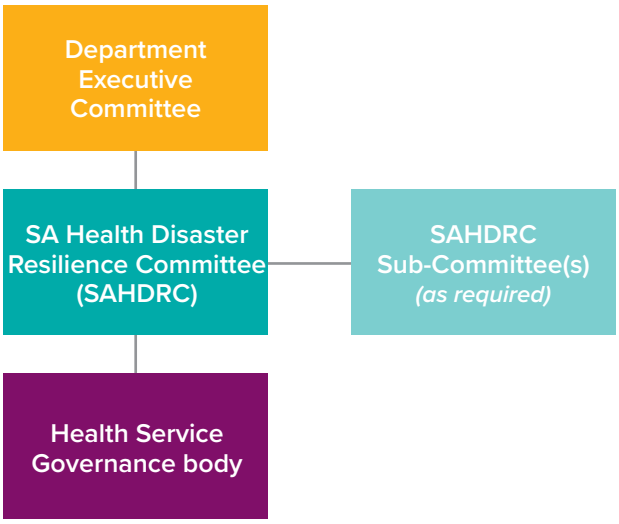


Figure 2 – SA Health Business Continuity Governance structure

SA Health Department Executive Committee, Chaired by the Chief Executive, SA Health will:

- responsible for disaster resilience policy and associated activities across SA Health, including BCM, and that appropriate BCM systems and processes are in place.

The SA Health Disaster Resilience Committee (SAHDRC) as a Tier 1 Committee will:

- provide strategic oversight of business continuity management policy and program activities
- provide strategic oversight and ongoing monitoring of compliance with the BCM Framework;
- provide regular reporting to Department Executive Committee about the BCM program, including assurance and compliance activities
- make recommendations to Department Executive Committee on the BCM program and any opportunities and/or barriers across SA Health.

Each Health Service (LHNs, State-wide Services, SAAS), as well as Digital Health SA and PSCM will:

- ensure there is an internal governance body to have oversight of BCM activities;
- oversee the implementation of the BCM Framework within their respective areas, including developing and maintaining effective plans and processes that are consistent with the BCM Framework, as well as training and exercising activities;
- undertake and report against assurance activities by the required timeframes;
- consider recommendations from SAHDRC on the implementation and maintenance of business continuity within their respective areas.

Roles and responsibilities

Chief Executive – SA Health

The Chief Executive (CE) of SA Health (and Chair of SA Health Department Executive Committee) has overall responsibility and management of South Australia's public sector health system. The CE will take reasonably practical steps to develop and issue system-wide policies applying to Local Health Networks, the SA Ambulance Service, and the Department for Health and Wellbeing. As such, the CE is responsible for ensuring that appropriate business continuity policy, assurance and reporting is in place to minimise the effects and impacts from business disruption related risks and ensure that SA Health can recover from a business disruption incident.

Local Health Network Governing Boards

LHN Governing Boards are responsible for the governance and oversight of business continuity risk, ensuring appropriate governance and systems are in place to oversee business continuity management plans, processes and reporting and that they are consistent with the BCM Framework. Boards will take reasonably practical steps to ensure that effective clinical and corporate governance frameworks (where relevant) are in place to ensure the LHNs are compliant with this BCM Framework.

Chief Executive Officers (LHNs, State-wide Services and SAAS), Chief Digital Health Officer, Digital Health SA and Executive Director PSCM

These roles are required to implement systems and process in line with the BCM Framework to ensure appropriate management of the effects and impacts from business disruption related risks. They also ensure that an appropriate person is identified and resourced to deliver on these BCM requirements (ie role of Business Continuity Management Coordinator).

Deputy Chief Executive Officers (DCE) and Executive Leads for Operating Entities or Attached Agencies (Wellbeing SA, Commission on Excellence and Innovation in Health) – DHW

Work with the DHW Business Continuity Program Manager (DPRB) on the following activities:

- review enterprise risk and business continuity risks identified in the BIA process
- participate in Strategic BCP development, approval and review annually
- participate in business continuity training/exercising, as required
- approve all BCM plans relevant to their business areas
- ensure that an appropriate person is identified and resourced to deliver on operational BCM requirements relevant to their business areas.

Business Unit Executive Directors and Directors – DHW

Work with the DHW Business Continuity Program Manager (DPRB) on the following activities:

- participate in operational BIA development and review annually, including discussion of business continuity risks
- participate in business continuity training/exercising, as required
- develop all required BCM plans (BIA, Operational BCP, ROC) relevant to their business area
- develop, monitor and review local arrangements, including local work instructions, compliance with BCM requirements and assurance activities
- assist in business continuity planning and exercising of the plans
- provide reports by the required timeframes against assurance activities
- review the currency and appropriateness of each business continuity plan relevant to their business unit / work area
- identify an appropriate person/s to coordinate BCM requirements

Business Continuity Program Manager – DHW (DPRB)

The key responsibilities of the Business Continuity Program Manager include:

- develop, promote and maintain the strategic policy for BCM (including the BCM Framework), ensuring that content is evidence-informed, contemporary and reflects best practice/lessons learned
- oversee and manage the BCM Program across SA Health, including monitoring its implementation and evaluating and reporting on its effectiveness
- implement the BCM Program for DHW, including undertaking risk discussions with key, designated staff and provide guidance, support and training in BCM activities
- coordinate, support and facilitate business continuity exercises for DHW
- support and advice to BCM Coordinators from LHNs, State-wide Services, SAAS, Digital Health and PSCM
- coordinate and manage annual assurance and compliance activities, and provide a summary report to SAHDRC, including evaluation of KPIs and compliance effectiveness

Note – This position is undertaken by the Senior BC and EM Officer, DPRB, DHW

Business Continuity Management Coordinator (BCPC)

The Business Continuity Management Coordinator from each Health Service (LHN, SAAS and State-wide Service, as well as Digital Health SA and PSCM) has the following responsibilities:

- coordinate, develop and maintain the Health Service BCM program requirements, including BIA, ROC and BCP plans.
- coordinate business continuity training and exercising arrangements
- coordinate and lead exercising of relevant plans
- record and report exercise results, including any resulting items
- participate in reviews of the business impact analysis annually
- review the currency and appropriateness of each business continuity plan relevant to their Health Service
- develop, monitor and review local arrangements, including local work instructions, compliance with BCM requirements and report by the required timeframes against assurance activities

Note – This position is usually undertaken by a BCM Coordinator, Health Service Risk Management Coordinator or an Emergency Management Coordinator or other nominated person/s within a Health Service.

Key Performance Indicators (KPIs)

The following KPI's have been developed to support the management of BCM across SA Health:

EXERCISE PLANS	Frequency	Compliance
ROC Plan	Every 12 months	100%
Operational BCP (Tier 1 & 2)	Every 12 months	100%

DOCUMENT REVIEW	Frequency	Compliance
BIA	Every 12 months	100%
Operational BCP (Tier 1 & 2)	Every 12 months	100%
ROC Plan	Every 12 months	100%
Strategic BCP	Every 2 years	100%
Post incident/exercise debrief report	Dedicated timeframe post incident, every 12 months (post exercise)	100%
Post incident/exercise Action Register	Dedicated timeframe post incident/ exercise, where necessary	As required

NB: the BCM Framework, Program and KPIs may meet, in part, evidence and accreditation requirements of the National Safety and Quality Health Service Standard 1, Action 1.10: Risk Management.

Culture

This framework aims to foster and support a business continuity and risk management culture that recognises and manages uncertainty relating to risks and recognises the value that risk management and business continuity brings to SA Health.

In doing so, it seeks to:

- encourage open, honest and transparent risk information
- support the identification and reporting of risks at all levels
- promote the consideration of broader risk and business implications.

It also aims to assist SA Health in recognition of risk management and business continuity management as an integral part of SA Health corporate and clinical governance frameworks.

The successful implementation of business continuity across SA Health and evidence of its value will be achieved through:

- ability to link risks with business objectives and processes
- embedding business continuity as part of the culture of decision making
- proactive risk identification rather than reactive.

Executive awareness and support

As already specified, LHN Boards, DHW Deputy Chief Executives and CEOs of Health Services are required to implement the BCM Framework across their respective business areas. They will define and communicate organisational objectives to assist with the prioritisation of resources in relation to Business Continuity efforts.

This will be further evidenced through proactive action, such as the allocation of relevant resources (human and physical) to undertake and maintain Business Continuity across the organisation, and identifying and resourcing BCM Coordinators for their area.

Executive level managers will also participate in BCP exercises or any identified training (if necessary).

Organisational awareness

Regular communication with staff will help to embed the processes and framework outlined in this document. Such communication can be supported by:

- appropriate business continuity training
- review and testing of all business continuity plans
- crisis management exercises
- discussions around the effectiveness of business continuity processes and their implementation
- encouragement of staff involvement in the business impact analysis
- post exercise or business disruption incident debrief and reports.

Analysis

Analysis within the BCM lifecycle reviews and analyses an organisation's objectives and functions and provides an assessment of key business disruption related risks that may enhance, prevent, degrade, accelerate or delay the achievement of operational objectives.

For SA Health, the BCM risk assessment and BIA analysis establish, implement and maintain a formal and documented process for business impact analysis and risk assessment that:

- Establishes the context of the assessment, defines criteria and evaluates the potential impact of a disruptive incident
- Takes into account legal and other requirements to which the organisation subscribes
- Includes systematic analysis, prioritisation of risk treatments, and their associated costs
- Defines the required output from the business impact analysis and risk assessment and specifies the requirement for this information to be kept up-to-date and confidential.

Figure 3 demonstrates how this is achieved both from a top down and bottom up approach:

The business disruption related risks should be considered as 'loss of' statements, for example:

- Loss of Workforce (human disease, weather event, industrial action)
- Loss of Supply chain / Logistics
- Loss of Building / accommodation (fire/earthquake/ flooding/weather event)
- Loss of essential services (gas / power / water / waste disposal)
- Loss of Telecommunications/ICT.

Importantly, within the context of SA Health, there are business disruption incidents that are not likely to cause an emergency incident, and similarly for an emergency incident to not cause a business disruption incident.

The table below demonstrates this:

Business disruption incidents		Emergency incidents
Disruption to the supply of essential services such as water / gas / power		Medical emergency (cardiac arrest / collapse etc)
Disruption to the access of a site (Industrial action / external emergency)		A small, contained fire
Disruption to the workforce (human disease / Industrial action)		A small – medium surge of patients to an LHN (car or bus crash)
Disruption to logistics, fleet, warehousing and supply chains	**VS**	Significant interstate or international incident that requires activation of national plans and additional patients being delivered to SA
Disruption to sanitation and waste management		Violent / aggressive client
Disruption to IT services (cyber-attack / hardware damage / power loss)		

Risk

The identification and assessment of business disruption related risks should occur in accordance with the *SA Health Risk Management Framework*.

It is essential that these risks are identified and captured on the relevant enterprise risk assessment registers. They should also be assessed and communicated to management to identify organisational vulnerabilities, and then also shared and discussed as part of business continuity risk and BIA discussions with BCM Facilitators/ Practitioners, and managed as part of annual plan reviews.

Importantly, risk assessment as part of business continuity considers the risk of disruption due to various threats, not just one.

The risk assessment phase will:

- Identify risks of disruption to the organisations prioritised activities and the processes, systems, information, people, assets, outsource partners and other resources that support them
- Systematically analyse risk, including consequence, likelihood and impact
- Evaluate which disruption related risks require treatment
- Identify treatments commensurate with business continuity objectives and in accordance with SA Health risk appetite
- Communicate known business disruption incident related risks, where applicable

For risks requiring treatments, consideration should be given to proactive measures that:

- reduce the likelihood of disruption
- shorten the period of disruption
- limit the impact of disruption on the organisations key services and products.

Business Impact Analysis (BIA)

The BIA is the cornerstone of any organisation's BCM program and is a mandatory component for SA Health. A business impact analysis (BIA) is undertaken on an annual basis, and/or when there is a significant re-structure to the DHW arrangements.

The BIA identifies, quantifies and qualifies the criticality of the processes, services and functions around SA Health, and determines how those that are critical can be supported during a significant outage. The BIA is not a risk assessment; rather it is an exposure assessment across multiple threats that will help drive the business unit response and recovery strategies.

Key objectives for a BIA phase are to:

- identify the critical functions and services across business areas
- assess the impacts over time of not performing these activities, and determine the maximum time service provision can continue to operate without a critical service or function before the impact will become unacceptable (known as the 'maximum acceptable outage - MAO')
- identify key resources (people, processes, systems) that are critical to continuing and recovering critical services and functions
- set prioritised timeframes for resuming these activities at a specified minimum acceptable level, taking into consideration the time within which the impacts of not resuming them would become unacceptable
- identification of all external and internal interdependencies across SA Health, including horizontal and vertical interdependencies, such as external services and suppliers
- identify manual workarounds or alternate working arrangements that are already in place for critical services or functions.
- a determination of the organisations capability to recover each critical service or function (recovery time objectives)
- measurement of the financial, operational and regulatory impacts associated with a disruption to critical parts of SA Health.

Prioritise Critical Business Functions (CBF's)

Part of the BIA process will separate out the various Tiers 1 and Tier 2 Critical Business Functions (CBF's). This prioritisation process will assist with the order in which to develop business continuity related response and recovery strategies to manage a disruption to the CBF and also assists with in which order to address CBF outages during a business disruption (response / recovery phase).

All SA Health CBF's rated as Tier 1 or Tier 2 require a BCP. For CBF's rated as Tier 3 or below a BCP is optional.

SA Health uses a CBF Prioritisation Matrix which is based upon the SA Health Risk Management Matrix as shown on the next page.

Critical Business Function (CBF) Prioritisation Matrix

Maximum Acceptable Outage	Non-Critical Business Function			Critical Business Function	
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Critical (5)
< 2 hours	Tier 4	Tier 4	Tier 3	Tier 1	Tier 1
2 – 24 hours	Tier 4	Tier 4	Tier 3	Tier 2	Tier 1
24 – 72 hours	Tier 5	Tier 4	Tier 3	Tier 2	Tier 2
> 72 hours	Tier 5	Tier 5	Tier 3	Tier 2	Tier 2

Impact Rating

NOTES

1. All business processes should be identified during the BIA stage and then prioritised according to the chart above (using the risk consequence table, as outlined with the *SA Health Risk Management Framework*)
2. Tier 1 & 2 are deemed to be "Critical Business Functions" for the purpose of the SA Health Business Continuity Framework
3. Tier 1 & 2 CBF's shall be then assessted and respective BC planning undertaken to mitigate risks to these processes and satisfactory workaround / response and recovery strategies.
4. Tier 3 – 5 should be reviewed and where the business unit identifies, BC planning shall be extended to these. If there is no specific requirement for workaround / strategies, then these processes shall be reviewed every 2 years as part of the 'normal' BC review cycle

STRATEGIC AND OPERATIONAL RISK ASSESSMENT MATRIX

CONSEQUENCE (Impact) RATING GUIDE

Level	Category	Clinical	Financial	Our People	Leagal, Policy and Regulatory	Organisation / Consumer	Corporate Reputation and Image
1	Insignificant	Negligible clinical event resolved without impact on Consumer or organisation	Financial loss of either less than $250,000 or 0.05% of budget	Negligible staff injury or near miss accident insignificant industrial grievance	Immaterial legal, regulatory or internal policy failure without penalty implication	Event with negligible impact on delivery of services to Consumers. Internal inconvenience only	One off negative media coverage only and no reputation impact
2	Minor	Clinical event resolved with minimal short term impact of Consumer or organisation	Financial loss of either between $250,000 to $1 million or between 0.05% to 0.2% of budget	Staff lost time injury. Local temporary poor engagement. Industrial grievance resolved internally	One-off minor legal, regulatory or internal policy failure resolved without penalty	Event with short term impact on delivery of services. Some impact on Consumers or Partners	Isolate adverse medial exposure. Temporary minor negative impact on reputation
3	Medium	Clinical event resulting in temporary injury of impact with considerable effect on Consumer or organisation. Internal investigation required. May require external mediation	Financial loss of either between $1 to $5 million or between 0.2% to 1% of budget	Temporary injury to staff. Ongoing widespread engagement issues. Industrial disputation mediated with no major penalty.	Repeated legal, regulatory or internal policy failure with penalty implications requiring internal investigation	Event requiring considerable remedial action with moderate impact on Consumers or Partners. Temporary loss of important information.	Repeated isolated negative reporting in media. Temporary breakdown in key relationship. Short term reputation damage.
4	Major	Clinical event resulting in serious permanent injury, requiring internal and medico legal investigation, external mediation, major penalties or compensation payments	Financial loss of either between $5 to $10 million or between 1% to 2% of budget	Serious permanent injury to staff. Entrenched engagement problems. Inability to recruit staff with necessary skills in key areas. Staff walkout and industrial stoppages.	Systemic legal, regulatory or internal policy failure with major penalty requiring extensive internal inquiry and external review	Event with major impact on delivery of services. Major impact on Consumers or Partners. Temporary loss of critical information	Widespread negative reporting in media leading to high-level independent investigation with adverse findings and longer term reputation damage. Premier or Ministerial involvement/ intervention by Cabinet. Breakdown in key relationship(s).
5	Critical	Failure in clinical governance processes/systems resulting in fatality requiring extensive internal and medico legal investigation, coroner's notification, significant penalties or compensation payments	Financial loss of either greater than $10 million or 2% of budget	Staff fatality, Simultaneous loss of a number of critical staff (e.g. Executive)	Substantial failure in internal governance and control structures resulting in Royal Commission and significant penalty	Event with significant impact on delivery of services across SA Health for an extended period. Significant impact on Consumers or Partners. Permanent loss of critical information.	Sustained adverse media exposure. Total loss of confidence within community and with the Government. Parliamentary enquiry. Serious long term impact on reputation.

NB: Financial impact is assessed in context of your Unit/Division/Department/Health Network/Service budget (funding allocation); the highest financial impact must be applied.

Firstly assess your IMPACT RATING

- Impact Rating - identify the most serious impact rating for the key business process being assessed (there may be several consequences identified, only the most serious / significant should be used for this assessment) – as per the SA Health Risk Management Framework.

Then assess your MAXIMUM ACCEPTABLE OUTAGE

- Determine the time frame in which an outage of the key business process will reach the Impact rating identified above.

The combination of these two determinants will identify a location on the matrix and identifies whether the key business process is a critical or non-critical process. It also assigns a 'Tier' rating to the process for the purpose of prioritisation.

Tier 3 – 5 are identified as non-critical business functions and should be identified as such, however minimal resources can be allocated to these unless the business function or Health Service requires.

Develop response and recover actions for Critical Business Functions

Within the BIA tool, information is collected about response and recovery actions. The key components for response and recovery actions are:

- critical business functions of SA Health
- short term workarounds and alternate working procedures and resources
- roles and responsibilities during a business disruption incident
- where there are interdependencies between business units or Health Services, these are identified and communicated
- identify and nominate any alternate / offsite work areas that may be required, either within a business area, Health Service or working from home (this needs to be collaborated at a higher level to ensure that there is no competition for the same resources by the organisation)
- triggers, activation, escalation and communication processes for when a BCP is invoked
- processes for resuming normal business operations within all levels of SA Health
- all critical services or functions are recovered according to agreed priorities as determined by the impact of their loss on the business
- the activities and resources required to support the continuity of critical services/functions and resumption of normal business operations is clearly defined
- responsibilities of relevant key management and staff
- key action steps to be followed and the strategic options and information required
- triggers for activation and guidance on when the Department should be informed or handed over to
- internal and external communication protocols
- dependencies for all in-scope components
- critical resources required and key contacts such as:
  - Emergency Services and external agencies.
  - The Department and other Health Services.
  - Digital Health SA Systems.
  - All relevant staff
  - External suppliers / contractors

Tier 3 – 5 business processes may be addressed if resources allow for it, or there is a specific business need. It may also be pre-determined that selective Tier 3 – 5 processes are intentionally reduced or ceased during a significant or prolonged business disruption incident.

Design

Design within the BCM lifecycle forms the strategy that connects appropriate response, continuity and recovery solutions for business disruption incidents to support critical business functions, stabilise the situation and recover to a business as usual state.

BCP approach

For SA Health, the design strategy involves the following key elements:

Business Impact Analysis (BIA)

As already discussed, the BIA identifies, quantifies and qualifies the criticality of the processes, services and functions around SA Health, and determines how those that are critical can be supported during a significant outage.

Operational Business Continuity Plan (BCP)

The Operational BCP is designed to be a key resource to support work areas, managers and staff with managing a significant business disruption incident through the provision of contextualised, specific actions and timely information to support the response and recovery arrangements for a critical business function. It contains response and recovery strategies, contact lists, resource requirements, relocation arrangements, communications plans and plan activation and notification authority. This plan will be used by staff, as well as incident management teams to ensure that business disruptions incidents are managed in a timely, safe and appropriate manner.

Resource Outage Contingency (ROC) Plan

The ROC Plan provides a high level overview of the relevant infrastructure vulnerabilities that could lead to a business disruption event for a particular site, such as the Citi-Centre building that houses DHW. It identifies the potential disruption (eg loss of ICT, Power, Water, Climate control, workforce and the building/premises itself) the vulnerability and impact each will have, as well as the response strategies.

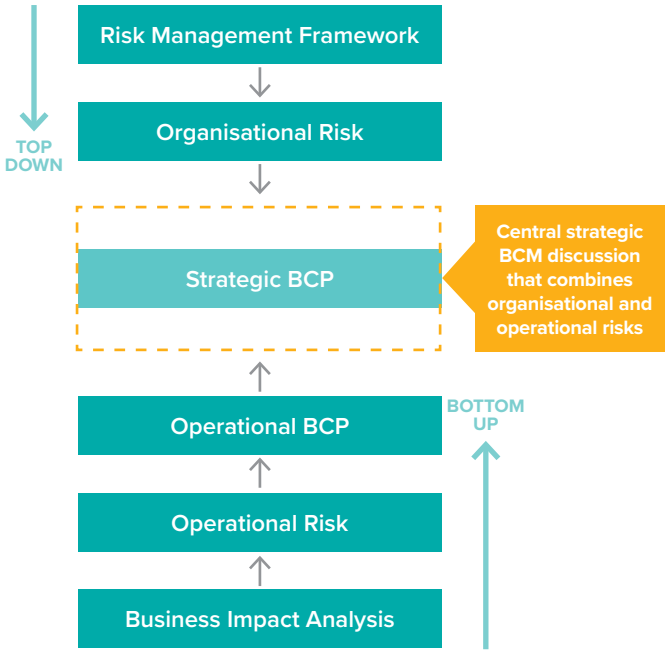
ROC Plans are developed in conjunction with DHW Infrastructure Services, as they have a critical role in identifying relevant sites that meet organisational and BCM requirements.

Strategic Business Continuity Plan (BCP)

The Strategic BCP provides a high level strategic overview of all identified critical business functions within a high level defined scope of responsibility such as DHW inclusive of all its organisational functions; or the RAH as a whole hospital; or PSCM inclusive of their Distribution Centre). Importantly, the Strategic BCP will also identify all relevant plans that sit under the Strategic BCP, such as the ROC Plan and Operational BCPs for all critical Tier 1 and Tier 2 critical services with an Operational BCP.

The Strategic BCP will be completed last, as the BCM Framework is both top down and bottom up, in its approach to business continuity discussions with Deputy Chief Executives or senior Health Service Executives. The figure below explains how the strategic business continuity discussion is informed from both the strategic (top down) and operational levels (bottom up). The Risk Management process is done at the Strategic level, and information identified here regarding business disruption risk should be included within BCM processes, similarly the operational aspects of the business to already have identified critical functions information to inform the central BCM discussion.

Figure 4 – BCM and Risk combined consultation and review – annual



Assess and activation

A BCP is enacted when normal or routine operations are no longer able to adequately support the business during a business disruption incident, and there is a need to initiate and implement non-routine arrangements to maintain critical business services.

Personnel responsible for activating BC Plans will be aware of their responsibilities and ensure that adequate reporting is undertaken when BC Plans are activated.

It is crucial that where a business disruption incident starts to impact upon multiple sites and / or multiple Health Services, that notification and alerting to the Department occurs in a timely manner. This provides mechanisms for a robust, consolidated and coordinated approach to managing the response and recovery to the business disruption.

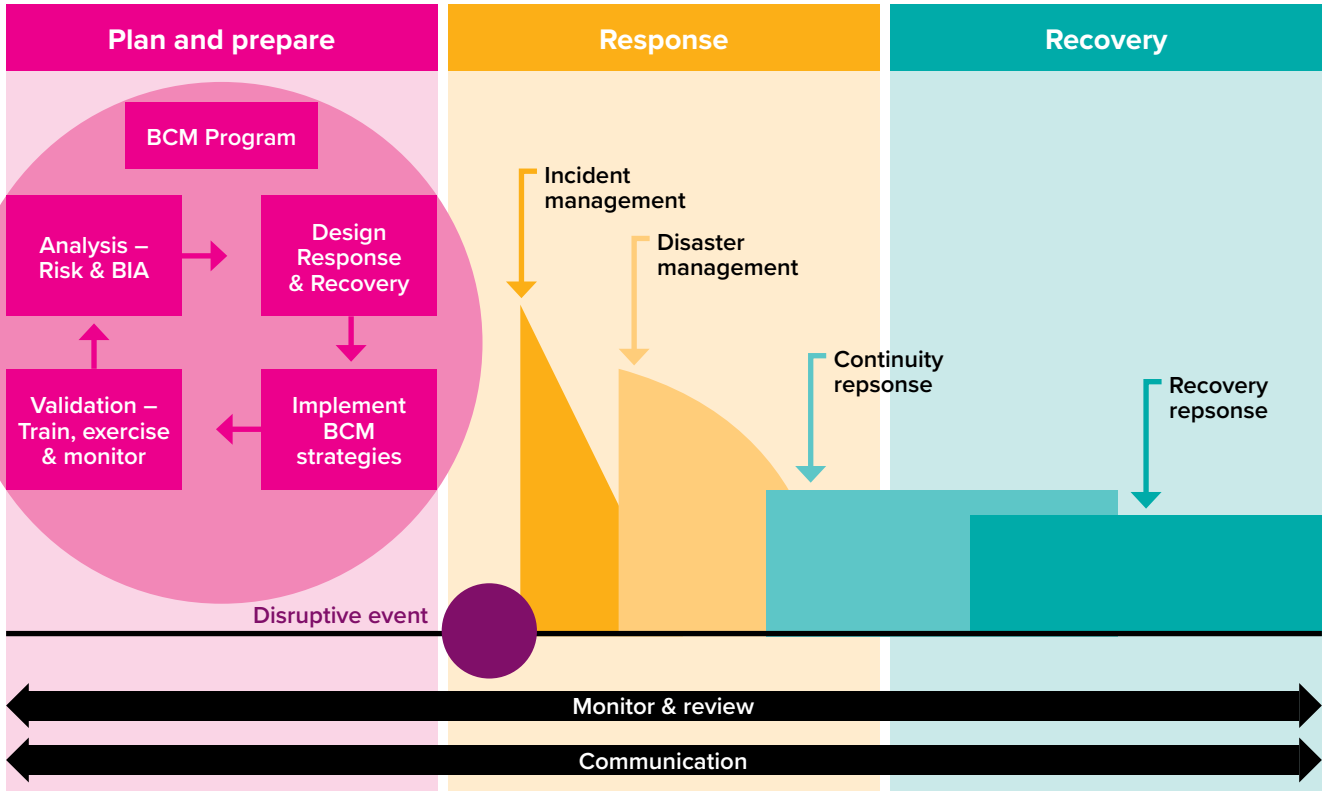
Additional considerations to the above table in relation to activation / escalation are:

- The maximum acceptable outage (MAO) of a critical service or function is likely to be exceeded.
- Agencies or government departments outside of SA Health and/or Emergency Services are involved.
- There will be a prolonged impact on the area which can cause downstream dependency problems.
- Loss of public confidence and/or public panic can result.
- The incident has political or reputation risks (actual or potential).

Response

The figure below illustrates the relationship between risk management, incident management and business continuity management and the interaction between the business continuity disciplines and their positioning in response to an incident.

Figure 5 – Relationship between RM, IM and BCM
(Source: adapted from Marsh & McLennan Companies)



Incident Management Response

The incident management response phase is primarily concerned with the preservation and protection of life and property in the immediate period following an incident. This phase is about reducing or ceasing any escalation / further risk of harm that may arise from the incident. This may also be termed as 'stabilising'.

Incident management response activities can range from an internal response, through to a coordinated evacuation plan with multi-agency support.

Disaster Management Response

The disaster management recovery phase is primarily concerned with strategic assessment and decision making following an incident. This phase is about organisation priorities, allocation of resources, communication and stakeholder management.

Disaster management response activities may include situation assessment of whether this poses a major and sustained disruptive threat to the organisation, determining the response strategy including resources, communicating decisions to the rest of the organisation and manage key stakeholder interests.

Business Continuity Response

The business continuity response phase is primarily concerned with providing a continuous and / or timely, yet potentially reduced level of output for each critical business function.

Similar to the Incident Management Response, it is crucial to reducing / ceasing any escalation / further risk of damage and harm that may arise from the incident.

Business continuity response activities can range from diversion of telephone services and invoking of Memorandums of Understanding (MoU) with other service providers through to a sophisticated and complex response strategy which considers entire or multiple DHW Divisions or Health Services.

The BIA should have identified the minimum workforce, physical, location and IT based resources required to provide output for the critical business functions affected by the business disruption incident.

Assumptions may relate to accommodation / premises expectations – several work areas all identify a single relocation site, however the site has limited capacity and will not accommodate everyone's needs.

Assumptions should be tested / exercised where they relate to response and recovery strategies to ensure that there are limited opportunities for critical failures.

Business Continuity Response – Communications

Communication strategies are paramount to ensuring that all relevant stakeholders are kept informed in a timely manner throughout a business disruption incident (BDI).

Any assumptions regarding ICT services and/or telecommunication capabilities (including mobile services), should be identified within the BIA.

Communication strategies should factor in potential loss of paging, internal and/or external telecommunications, ICT services (email etc) and mobile telecommunications.

Communication considerations include (but not be limited to):

- Alerting / Notifying key personnel of a business disruption incident.
- Communication updates / advice regarding BC response and recovery strategies to a wider range of people, including:
  - Internal staff.
  - External sites.
  - Third party contractors / suppliers.

Where media releases are required to assist with messaging to support BC response and recovery arrangements, then advice should be sought through relevant media communications staff.

Business Continuity Recovery

The business continuity recovery phase is primarily concerned with the transition of the affected areas to a business as usual (BAU) state. This phase is longer term as it considers the acceptability and sustainability of the impact areas and their ability to transition and resume operational activity to BAU.

Much of the recovery phase can be pre-planned, however it is important to note that some of the planning can only occur once the incident has occurred and the extent and nature of the damage is evidenced. Plans can be adapted to support the required (and agreed) response strategy to first stabilise and then restore the disrupted functions.

It is hoped that as a part of the business continuity response and recovery actions, and a subsequent debrief and follow up, that a culture of resilience can be built into the organisation.

BCP documentation

The table below outlines the key documentation that should be in place within SA Health and who is responsible:

Business area	Responsibility / Approval	Frequency
BIA		
Department for Health and Wellbeing (DHW)	Executive Directors / Directors of Business Units within each Division / Operating Entities	Every 12 months
Digital Health SA	Executive Director, Digital Health SA	Every 12 months
PSCM	Executive Director, PSCM	Every 12 months
Health Services (LHNs, SAAS and State-wide)	Executive Directors / Directors of Business Units within each relevant area	Every 12 months
Operational BCP		
DHW	Executive Directors / Directors of Business Units within each Division / Operating Entities	Every 12 months
Digital Health SA	Executive Director, Digital Health SA	Every 12 months
PSCM	Executive Director, PSCM	Every 12 months
Health Services (LHNs, SAAS and State-wide)	Executive Directors / Directors of Business Units within each relevant area	Every 12 months
ROC Plan		
DHA Citi-Centre Building , and other relevant infrastructure	Executive Director Infrastructure and Chief Executive	Every 12 months
Digital Health SA	Executive Director, Digital Health SA	Every 12 months
PSCM Distribution Centre	Executive Director, PSCM	Every 12 months
Health Services (LHNs, SAAS and State-wide)	Chief Executive Officer	Every 12 months
Strategic BCP		
DHW - overall	Chief Executive, SA Health (endorsed by each DCE / Executive lead for Operating Entities)	Every 2 years
DHW Division / Operating Entities	DCE / Executive lead for Operating Entities	Every 2 years
Digital Health SA	Executive Director, Digital Health SA	Every 2 years
PSCM	Executive Director, PSCM	Every 2 years
Health Services (LHNs, SAAS and State-wide)	Chief Executive Officer and Executive Directors / Directors of Business Units within each relevant area	Every 2 years

BCP documentation should contain the following information:

Business Impact Analysis (BIA)

As already discussed, the BIA identifies, quantifies and qualifies the criticality of the processes, services and functions around SA Health, and determines how those that are critical can be supported during a significant outage.

Upon completion, the BIA based upon the CBF Prioritisation Matrix highlights Tier 1 and Tier 2 critical business functions, along with Tier 3-5 critical business functions, key dependencies and alternate working arrangements and enables business continuity solutions and mitigation measures to be designed.

The BIA is mandatory.

Operational Business Continuity Plan (BCP)

As already mentioned, the Operational BCP is designed to be a key resource to support work areas, managers and staff with managing a significant business disruption incident through the provision of contextualised, specific actions and timely information to support the response and recovery arrangements for a critical business function.

The Operational BCP will focus on every Tier 1 and Tier 2 critical functions identified in the BIA process (the BIA may record other functions, these are not mandatory to be included in the resulting Operational BCP)

The Operational BCP is mandatory.

Resource Outage Contingency (ROC) Plan

As mentioned earlier, the ROC Plan provides a high level overview of the relevant infrastructure vulnerabilities that could lead to a business disruption event for a particular site. The key objective of the ROC Plan is to manage an incident that affects multiple services or functions.

ROC Plans are developed in conjunction with DHW Infrastructure Services, as they have a critical role in identifying relevant sites that meet organisational and BCM requirements.

DHW will ensure that there is a ROC for its Citi-Centre Building, as this is where a large concentration of its services and critical business functions are. DHW Infrastructure Services will determine ROC Plan requirements for other relevant DHW infrastructure/locations.

A separate ROC Plan will be developed for the following DHW responsible entities (owing to their size, geographical spread and/or complexity) and not limited to any single, specific site:

- Digital Health SA
- PSCM Distribution Centre

The ROC Plan is mandatory.

Strategic Business Continuity Plan (BCP)

As mentioned earlier, the Strategic BCP provides a high level strategic overview of all identified critical business functions within a high level defined scope of responsibility.

The Strategic BPC should include:

- Purpose and context for the plan
- Who has authority over the plan, audience and distribution
- Any assumptions and limitations
- Overview of all the associated ROC and Operational Plans that sit within the remit of the plan, and where these plans are located.

The Strategic BCP is mandatory.

Local work instruction

Where non-critical business functions are identified through the BIA process, such as Tier 3-5 business functions, then a local work instruction/documentation may be required. Local managers will determine whether there exists a need for a local work instruction(s) based upon their criticality rating from the BIA. These are designed to describe any local arrangements in response to a business disruption incident.

These will be developed and stored locally within the business unit at an operational level.

Control of documentation

All documents should be stored appropriately according to the *SA Health Corporate Records Management Policy Directive*, including the appropriate electronic document records management system (EDRMS), such as eObjective.

All documents must be approved by the relevant owner, inclusive of appropriate signature approvals, and a PDF version created as the single source of truth. Copies of this single source can then be utilised in the following ways:

- uploaded into the "Document Repository" of the SA Health Emergency Management System (SAHEMS), for ease of access during an incident, as SAHEMS is the mandated incident management system across SA Health and allows 24/7 access.
- hard copies and electronic copies of the single source should be provided to all owners, managers, incident teams and responsible executives to ensure they have access to all plans both during and outside of work hours.
- Local versions of documents and local work instructions are clearly updated and local historical copies are removed and destroyed.
- Consideration should also be given to a back-up box/ battle box that contains hard copies of all plans, and other useful items for use during a business disruption event, such as torches, batteries, USBs, ICT charges, etc. These should be easily accessible during an Incident.

In addition, an electronic and accompanying hard copy will be supplied to the following key staff;

- SA Health Chief Executive
- Deputy Chief Executive(s) and/or Chief Operating Officers
- Executive/Group Directors and/or Unit Managers
- Service and Site Commander(s)
- DHW Emergency Management Unit (electronic only through SAHEMS)
- All BCP owners
- Fire Control Panel (via Police Security Services Branch (PSSB) personnel)

Validation

Training, exercising and assurance regimes ensure familiarity with plans, confidence in response activities during an incident and that the dependent resources and departments (such as infrastructure, IT, workforce and communications) support the business recovery strategies and are aligned with all plans in place.

Training

All levels within SA Health should have an understanding and appreciation of what they should undertake during a business disruption event and the importance of business continuity in providing this understanding. At a minimum, all levels should aim to have:

- General overview of business continuity management principles and this BCM Framework
- familiarity with their respective BCM plans (BCP, ROC, etc)
- annual record of attendance at any training and exercising, as per BCM Framework KPIs

DPRB, DHW, will develop any training identified in the *SA Health Disaster Resilience Training and Exercising Framework*.

Exercising

All Operational BCPs and ROC plans should be exercised annually. This should comprise a scenario based discussion exercise as a minimum. Please see definitions for exercises and other relevant exercise information in the SA Health Disaster Resilience Training and Exercising Framework.

It is strongly encouraged to incorporate BC exercising / scenarios into broader emergency management related exercises. This further raises the profile of business continuity, as well as highlights possible interdependencies between resources (human or physical) during emergency and business disruption incidents. Importantly, there should still be a focus on exercising the BCP, validating the processes for identified critical business functions and minimising the effects or recovering from a business disruption event, as part of any combined exercise.

It may also be relevant to undertake joint exercises with Suppliers, particularly those who hold facility management contracts at major hospitals, or deliver services on behalf of SA Health, such as out of hospital care.

Local work instructions may also be exercised, but this is not compulsory.

The DPRB, DHW will assist with exercise facilitation for DHW, along with other training identified in the SA Health Disaster Resilience Training and Exercising Framework. Each Health Service is required to develop an exercise schedule that includes all plans, and report on this to their relevant governance committee and annually as part of assurance activities undertaken by the DPRB.

A post exercise debrief outlining lessons learned and areas for improvement should be undertaken within 6 weeks of each exercise and any gaps or opportunities identified from the exercises should be captured and an Action Register developed, with individuals assigned to address arising tasks. The relevant governance committee should monitor progress of the Action Register.

Post incident debrief

A post incident debrief will be conducted following any significant business disruption incident.

A formal debrief should occur no more than 6 weeks post a significant business disruption incident and reported to their respective Governance Committee.

The formal debrief should focus on the systems and processes of the organisation and the effectiveness of the relevant plans and planning process. Debriefs should avoid focus on individuals, however an outcome from a debrief process may recommend greater training for key personnel.

Any lessons learned, recommendations or gaps, should be captured and an Action Plan be developed to improve and build both resilience and capability, with a view to 'learn' from the incident.

A summary may also be provided the DPRB and to the respective Disaster Resilience / Risk & Audit / Corporate Governance Committee.

Monitoring and Review

All levels of SA Health should adopt sound continuous improvement practices to ensure that the business continuity capability is continually maintained, tested and re-assessed across SA Health.

This can be achieved by building in mechanisms such as:

- implementing a continuous monitoring regime of all BCM program strategies, which ensures that changes in business processes and to the supporting infrastructure are captured.
- maintenance schedules for plans.
- ensuring the correct governance and ownership of the business continuity documents and processes (particularly within each Health Service) is allocated and maintained accordingly.

Assurance

Compliance with the BCM Framework will be measured through regular qualitative reporting, annual system wide reviews and periodic internal audits. The details are as follows:

Regular reporting and annual BCM Self-assessment - led by Disaster Preparedness and Resilience Branch, DHW

DPRB will coordinate regular reporting for BCM activity to be tabled at each SAHDRC meeting. This will involve the following:

- The most recent BCM status reports from LHN/SAAS/ SCSS/Digital Health/PSCM to their respective Disaster Resilience / Risk & Audit / Corporate Governance Committee that oversees BCM activity. These reports will be submitted to DPRB in line with SAHDRC paper submission deadlines.
- An annual self-assessment survey will be completed by BCM Coordinators (across SA Health) and submitted to the DPRB who will compile, analyse and evaluate the data. The Summary Report will be provided to SAHDRC for review and approval of any recommendations. A copy will also be provided to SA Health Department Executive Committee for noting. Any identified gaps or opportunities identified will be placed into a BCM Framework Action Register for monitoring and follow up by DPRB/SAHDRC.

Three to five years – Formal Audit - led by Risk and Assurance Services, DHW.

A three to five year cycle of audits will be undertaken by Risk and Assurance Services, DHW.

Any identified gaps or opportunities identified in the audit will be placed into a DHW Risk/Audit Action Register (by Risk and Assurance Services) for monitoring and follow up.

Hospital Accreditation

It should be noted that the BCM Framework, Program and KPIs may meet, in part, evidence and accreditation requirements of the National Safety and Quality Health Service Standard 1, Action 1.10: Risk Management.

For more information

Disaster Preparedness and Resilience Branch
Health Regulation and Protection
SA Health

Email: HealthEmergencyManagement@sa.gov.au
Telephone: (08) 7425 7065
sahealth.sa.gov.au

Confidentiality-I2-A2

https://creativecommons.org/licenses

Government of South Australia

SA Health