Business Continuity Plan

Australian Catholic University

Version 1.0

April 2024

Document Control

Effective date	1 May 2024
Review date	1 May 2026
Responsible area	Corporate Services Portfolio
Approved by	Chief Operating Officer
Distribution	• Senior Executive • Portfolio Executives
Version number	1.0

Table of Contents

Introduction and Overview

Australian Catholic University (ACU) is committed to enabling the timely recovery of its own Critical Business Functions and systems should a disruption affecting ACU occur. The Business Continuity Plan (BCP) has been developed to support this intent and is underpinned by ACU's Business Continuity Policy and Framework.

This BCP describes the actions required to respond and recover time-critical business activities following a serious disruption impacting ACU's ability to continue its operations.

A disruption is considered serious where the Incident or may not be managed via business-as-usual arrangements, and the Incident has affected (or has the potential to affect):

- day-to-day operations;
- the health and safety of staff, students, contractors or visitors; and/or
- the reputation of the University; and/or the community.

Scope

The scope of this plan includes:

- Learning and teaching
- Research
- Enabling operational services

Purpose and Objectives

The purpose of the BCP is:

- o To provide a structured approach to recovering from an Incident or Critical Incident.
- o To identify the essential operational elements (including interdependencies), staff, systems and resources required to be maintained in the event of a business interruption/incident.
- o To minimise/control potential impacts of threats on business operations and systems.

Our business continuity objectives are to:

- o Minimise the impact on people, including staff, students and members of the community.
- o Minimise potential safety issues in a non-standard operating environment.
- o Minimise disruption to operations and continuity of services.
- o Minimise Financial, Education, Reputational, Governance, Strategic and Community Wellbeing impacts to ACU.

Plan Integration

The below diagram is a graphical representation of the Business Resilience Framework hierarchy and the integrations with other plans and processes across the University.
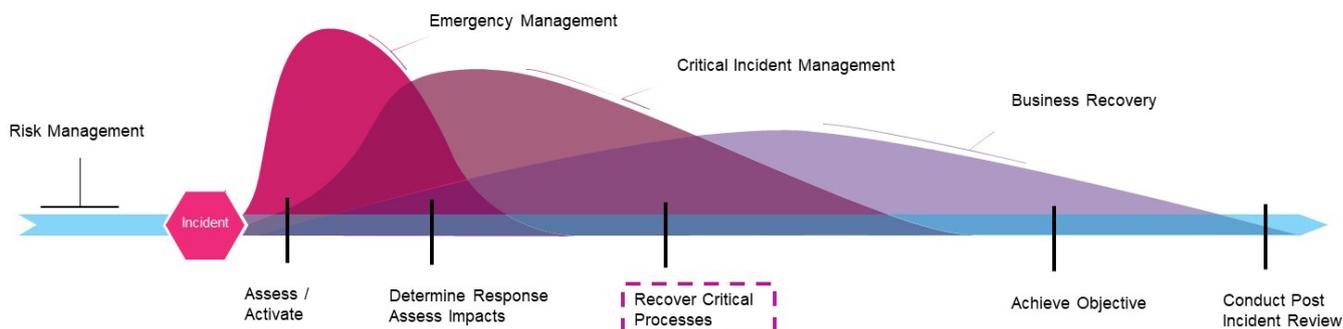
Risk Management Plan – Documented potential risks to ACU, and the steps that should be taken to keep those risks at acceptable levels.

Emergency management – Provides structure to the Emergency Control Organisation in how to manage an immediate response to emergencies across ACU, including evacuations and lockdowns.

Critical Incident Management – Documented policies and processes to manage an Incident or Critical Incident, reducing impacts to people, assets, financial, reputational, operational and strategic outcomes.

Business Continuity Plan – Documented procedures guiding the Critical Incident Response Group (CIRG) and Business Recovery Lead in how to recover, resume, and restore to a pre-defined level of operation for whole of University following a serious Incident.

Business Recovery Plan – Portfolio specific guidelines and template for use by the Senior Exective Members in how to recover, resume and restore to a pre-defined level of operation for their organisational unit.

Business Resilience Flowchart

The following flowcharts shows the process workflow from start to finish with managing a serious incident.

```
                          ┌─────────────────┐
                          │  Incident or    │
                          │  disruptive     │
                          │  event          │
                          └────────┬────────┘
                                   │
                                   ▼
                          ╱─────────────────╲         ┌─────────────────┐
                         ╱  Threat to life    ╲  Yes   │ Confirm safety  │
                         ╲  and/or property?  ╱───────▶│ and welfare of  │
                          ╲─────────────────╱         │ staff, students │
                                   │ No               │ and visitors    │
                                   ▼                  └────────┬────────┘
   ┌──────────────┐       ┌─────────────────┐                 │
   │  Assessment  │◀──────│ 1. Determine    │◀────────────────┘
   │  Tool        │       │ extent of       │
   └──────┬───────┘       │ disruption      │
          │               └────────┬────────┘
          ▼                        ▼
   ┌──────────────┐       ╱─────────────────╲                  ┌──────────────┐
   │ Loss of      │       ╱  Disruption       ╲   No           │ Stay alert   │
   │ people,      │┄┄┄┄┄▶ ╲  to critical      ╱───────────────▶│ and monitor  │
   │ buildings,   │       ╲  services?        ╱                └──────────────┘
   │ IT, supplier │        ╲─────────────────╱
   └──────────────┘                 │ Yes
                                    ▼
   ┌──────────────┐       ┌─────────────────┐
   │ Business     │◀──────│ 2. Activate     │
   │ Continuity   │       │ Business        │
   │ Plan         │       │ Continuity Plan │
   └──────────────┘       └────────┬────────┘
                                   ▼
   ┌──────────────┐       ┌─────────────────┐
   │ Business     │◀──────│ Activate        │
   │ Recovery     │       │ Business        │
   │ Plans        │       │ Recovery Plans  │
   └──────────────┘       └────────┬────────┘
                                   ▼
   ┌──────────────┐       ┌─────────────────┐
   │ Recovery     │◀──────│ 3. Activate     │
   │ Lead         │       │ Business        │
   │ Checklist    │       │ Recovery Lead   │
   └──────────────┘       └────────┬────────┘
                                   ▼
   ┌──────────────┐       ┌─────────────────┐
   │ Recovery     │◀──────│ 4. Select       │
   │ Strategies   │       │ Recovery        │
   └──────┬───────┘       │ Strategy        │
          │               └────────┬────────┘
          ▼                        ▼
   ┌──────────────┐       ┌─────────────────┐
   │ Loss of      │       │ Activate        │
   │ people,      │       │ Recovery        │
   │ building,    │       │ Support         │
   │ IT, supplier │       │ Procedures      │
   └──────────────┘       └────────┬────────┘
                                   ▼
                          ┌─────────────────┐
                          │ Recover         │
                          │ critical        │
                          │ business        │
                          │ functions       │
                          └────────┬────────┘
                                   ▼
                          ┌─────────────────┐
                          │ Conduct After   │
                          │ Action          │──────────────────┐
                          │ Review          │                  │
                          └─────────────────┘                  │
                                              (to Stay alert and monitor)
```

Structure of this Plan

This document covers the key phases of a serious incident including:

1. Identifying and stabilising the situation
2. Recovering Critical Business Functions
3. Implementing business resumption

Responses to Incidents at ACU will be conducted in accordance with existing emergency management and Critical Incident Management procedures. This includes the activation of the Critical Incident Response Group (CIRG) as required. This Business Continuity Plan (BCP) may be activated and used concurrently with emergency management processes and Critical Incident Management plans being used.

Once a critical incident has been declared, a Business Recovery Lead may be appointed to assess business operational impacts resulting from the disruption and activate the Business Continuity Plan. In doing so, they must continue to follow all instructions from the Critical Incident Convener and CIRG.

Following a major disruption affecting business functions, the Business Recovery Lead will be expected to manage the recovery of Critical Business Functions per the procedures and processes in this Business Continuity Plan and Business Recovery Plans. A brief overview of each section is provided below.

Phase 1: Identify and stabilise the situation

This section provides a protocol for stabilising the situation. It includes a list of immediate actions that should be performed by ACU personnel, incident assessment tools, contact lists, key roles and responsibilities.

Phase 2: Recover Critical Business Functions

This section includes a series of strategies designed to enable the recovery of Critical Business Functions immediately following a business interruption.

Recovery strategies have been developed for the following events:

- Loss of Key People
- Denial of Access to Premises (Temporary / Permanent)
- Sustained Failure of IT infrastructure and communications systems
- Loss of Critical Service Provider
- Loss of Research

The Business Recovery Plans also provides supporting information including critical business function lists, relocation schedules and minimum resources required to support the implementation of recovery strategies for Portfolios and their organisational units.

Phase 3: Implementing Business Resumption

This section includes a checklist to assist the Business Recovery Lead in moving ACU to an operating state that existed prior to the interruption. This may include the ACU team member working from their normal location, moving operations to alternate permanent premises, increasing staffing to pre-interruption status, liaising with the insurance company to access coverage and make claims, and communicating with relevant stakeholders regarding the movement to 'business as usual'.

Roles and Responsibilities

Business Recovery Lead checklist

This checklist will guide the **Business Recovery Lead** / Critical Incident Response Group (CIRG) on the actions required to prepare for responding to a serious incident. The Business Recovery Lead will support the CIRG during business recovery and business resumption phases. The Business Recovery Plans will not have a checklist for the Business Recovery Lead given there is one Lead for the whole of ACU.

Pre-disruption Actions

Step	Task	Done
1.	Identify and ensure Critical Incident Response Group members are fully trained to fill the Business Recovery Role.	☐
2.	Ensure recovery procedures, resources and facilities are readily available.	☐
3.	Ensure the Business Continuity Plan and Business Recovery Plans are updated regularly.	☐
4.	Ensure Business Impact Analysis are developed and updated regularly.	☐
5.	Liaise with IT to ensure IT have an up-to-date IT Incident Management Process which is tested. Ensure RTOs align with recovery requirements for ACU.	☐
6.	Monitor agreements with key suppliers to ensure continuity arrangements are considered.	☐
7.	Ensure the Business Continuity Plan and Business Recovery Plans are accessible to the Business Recovery Lead, and leaders of Portfolios and organisational units.	☐
8.	Ensure that a copy of all contact details of employees is available and accessible if systems are not functioning.	☐

Business Recovery

The following checklist should be used by the Business Recovery Lead to resume organisation operations.

Step	Task	Done
1.	Gather information and determine facts of the disruption. o What has happened? o What is the current status? o How long is the disruption expected to last? o What is happening to contain / resolve the incident?	☐
2.	Ensure welfare of staff and students is confirmed and any injuries or welfare issues communicated to the CIRG.	☐
3.	Should persons be in danger or injured, ensure emergency management procedures have been activated.	☐
4.	Determine extent of disruption by using the <u>Step 2: Determine extent of disruption using Assessment Tool</u>. Communicate outcome to Critical Incident Response Group.	☐
5.	Commence a physical damage assessment to determine likely downtime estimate. This should include:	☐

Step	Task	Done
	o IT equipment including software applications;	
	o voice and data communications;	
	o buildings'	
	o uilities (gas, water, electricity);	
	o equipment; and	
	o other ACU buildings in the area, if the damage is widespread.	
6.	Ensure task logs are maintained.	☐
7.	Declare a business continuity (Chief Operating Officer and Critical Incident Convener).	☐
8.	Notify those needing to be activated to assist with the business recovery processes. This may include: o Critical Incident Response Group o Business Continuity owners o Portfolio executives and organisational unit leads	☐
9.	Conduct an Impact and Issues Assessment (refer Appendix C – Impact and issues assessment)	☐
10.	Operate through an MS Teams Channel if it has been established. Refer to the Critical Incident Management Procedure.	☐
11.	Facilitate communications between the Critical Incident Response Group and other key stakeholders as part of the business recovery process.	☐
12.	Review the current financial position, if needed.	☐
13.	Provide an update of impact and issues assessment to the Critical Incident Convener.	☐
14.	If voice communications are affected, ensure phones are diverted, and confirm functionality.	☐
15.	Determine recovery strategy to be implemented. Recovery Strategy # 1 – Loss of Key People Recovery Strategy # 2 – Failure of IT/Comms Recovery Strategy # 3 – Denial of Access to Buildings Recovery Strategy # 4 – Failure of Material / Critical Service Provider Recovery Strategy # 5 – Loss of Research	☐
16.	Review summary of Critical Business Functions list to assess all work-in-progress affected by the disruption. Refer to Appendix D – Critical Business Functions for the list of Critical Business Functions within a Recoverable Time Objective of 24 hours. Refer to Business Recovery Plans for the detailed Critical Business Functions at an organisational unit level.	☐
17.	If extended downtime is estimated (greater than 24 hours), determine need to initiate activation of relocation plan for essential staff. For offsite relocations, liaise with site manager to confirm location and resources are available.	☐
18.	If key staff members have been affected, determine if work can be covered by existing staff. If not, activate workarounds for affected Critical Business Functions. Actions for other parties should be documented using Appendix E – Briefing Template.	☐
19.	Develop a **communications strategy** including stakeholder, frequency, key messaging etc. Chief Marketing Officer to oversee and coordinate release of the communications.	☐
20.	For any disrupted Critical Business Functions identify: o how workarounds will be implemented (refer recovery strategies); o staff that need to be relocated to alternate sites or to work from home; o availability of IT access for staff to work from alternate sites and/or home;	☐

Step	Task	Done
	○ communication requirements for staff, visitors and affected third parties; ○ transportation requirements for staff that need to be relocated; and ○ additional resources required to support on-going recovery.	
21.	Provide the Business Recovery Lead with an update on the impact, and recommended actions.	☐
22.	Facilitate relocation of essential staff (where required) to established alternate locations. Advise all other affected staff (who are not currently working remotely) to return home until further notice, if advised so by the Critical Incident Convener.	☐
23.	Develop any new operational procedures and instructions required because of the temporary operating environment.	☐
24.	Confirm who can authorise additional expenditure (per the ACU Financial Delegations). Keep records of all expenditure.	☐
25.	Work with the relevant procurement team (eg properties, IT) to procure replacement equipment and fixtures as determined by damage assessment.	☐
26.	If damaged site/s is accessible & deemed safe, organise for retrieval of key documentation and/or equipment.	☐
27.	Provide regular status report to CIRG on critical business capabilities.	☐

Phase 1: Identify and stabilise the situation

Step 1: Identify a potential situation and collect information

Any ACU team member becoming aware of a possible Incident or Critical Incident must notify the Critical Incident Response Group through the National Security Centre (NSC). The Incident Convener will use the information collection tool (refer Appendix B) to capture the initial information and move to the next step being to determine the extent of the Incident.

Step 2: Determine extent of disruption using Assessment Tool

The Business Recovery Lead will use the following tool to identify whether the Business Continuity Plan should be activated based on the likely impact and the disruption timescale. The likely impact is determined in collaboration with organisational units.

Following completion of this assessment, the Business Recovery Lead will determine likely impacts and suggested recovery options. On activation of the BCP, the Business Recovery Lead will provide updates to the Critical Incident Convener. The Critical Incident Convener will determine if an Incident will be escalated to a Critical Incident.

Note: this tool is used for determining activation of the Business Continuity Plan at a University level. If a Business Recovery Plan has been activated, the event may not necessarily require activation of the Business Continuity Plan at University level.

Event Statement	Yes	No
Loss of people (unavailable to work), impacting Critical Business Functions.	If yes to any of the questions, activate the **Business Recovery Lead** and **Business Continuity Plan**	If no, maintain business as usual operations and monitor the situation until resolved
Facilities or infrastructure rendered unusable, impacting Critical Business Functions.		
Equipment rendered unusable, impacting Critical Business Functions.		
Utilities including back-up power, water, gas, etc has been disrupted, impacting Critical Business Functions.		
IT and/or comms services has been disrupted resulting in impact to Critical Business Functions.		
A critical supplier lost where there is a dependency, impacting Critical Business Functions.		

Step 3: Decision on activating the Business Continuity Plan

The decision to activate the BCP sits with the **Critical Incident Convener.**

Activation of the Business Continuity Plan will involve notification to each member of the Critical Incident Response Group.

The BCP may also be activated in conjunction with related processes (such as Emergency Management, Critical Incident Management, IT Incident Management) as well as Business Continuity Plans of key suppliers.

Step 4: Activate Business Recovery Lead

The activation of the BCP will activate the Business Recovery Lead. The Business Recovery Lead is responsible for working with organisational units to recover Critical Business Functions.

The Business Recovery Lead will report to the Critical Incident Response Group and the Critical Incident Convener.

Refer to the Critical Incident Management Procedures for other team roles.

Critical Incident Response Group

Type	Convener	Proxy	Support
Critical Incident Convenor	Chief Operating Officer & Deputy Vice-Chancellor	Deputy Chief Operating Officer	Portfolio Executive Officer
Students	Academic Registrar and Director, Student Administration	Associate Director Administrative Services	Executive Officer, PHS Corporate Services
Staff	Chief People Officer	Associate Director, HR Business Partnering & Talent Management	Executive Officer, PHS Corporate Services
Physical	Director, Properties & Facilities	State Facilities Manager (VIC/SA)	Executive Officer, PHS Corporate Services
Virtual	Chief Information Officer	Associate Director, Service Delivery, IT Client Services	Executive Officer, PHS Corporate Services
Reputation	Director, Marketing and External Relations	Associate Director, Communication and Creative Services	Executive Officer, PHS Corporate Services

Other CIRG members
• Program Officer, Office of Deputy Chief Operating Officer • Chief Financial Officer • State Facilities Manager (QLD/ACT) • State Facilities Manager (NSW) • State Facilities Manager (VIC/SA) • Associate Director, Communication and Creative Services (Reputation Convener Proxy) • National Manager, Strategic Communications
Incident Conveners can select and approve any ACU member staff for inclusion in an **Incident Response Group.** Staff who are members of the Incident Response Group provide expertise and resources to support the Incident Convener and are selected based on the Incident type, colour code and campus.

Phase 2: Recover Critical Business Functions

Recovery Strategies

The following recovery strategies were identified through the Business Impact Analysis process. These strategies are focused on recovery of disruptions. The Business Recovery Lead will determine the recovery strategy to be adopted.

Note: the timings below are referencing the timeframes after the business continuity phase is initiated. Business Continuity is activated after the activation of the Critical Incident Management Policy and Emergency Management processes if they have been activated. The welfare of staff is considered the utmost priority and will be attended to as first priority.

Recovery Strategy # 1 – Loss of key or large number of people

Where a person with a key dependency is not available, or large number of persons will not be available, impacting on the ability for ACU to deliver Critical Business Functions.

Step	Timing	Activity/Action/Task	☒
1.	0-2 hrs	If there was an emergency affecting people welfare, ensure people are safe and accounted for.	☐
2.	2-4 hrs	Determine extent of loss of persons – number of persons, estimated time away, organisational units impacted.	☐
3.	4-12 hrs	Review the critical business function listings in Appendix D and assess all work-in-progress affected by loss of employee/s for Critical Business Functions.	☐
4.	4-12 hrs	Review organisational Units where there is a reliance on key individuals. If those individuals are unavailable, consider alternate measures for those affected Critical Business Functions. The following functions are the Critical Business Functions at a strategic level that will be the focus for the first 24 hours. ○ Management of critical incidents ○ AskACU call taking ○ ServiceCentral call taking ○ Student Administration enrolment processing ○ Student accommodation ○ Facility management of critical property matters ○ IT communication systems	☐
5.	4-12 hrs	Determine if work can be covered by existing employees. If not, transfer affected functions to other staff or industry experts as appropriate.	☐
6.	4-12 hrs	Determine corporate knowledge loss.	☐
7.	4-12 hrs	Assess requirement to use casual employees, contact an agency for temps or contact industry experts as required.	☐
8.	4-12 hrs	In the case of serious injury or death, work with the CIRG and the Chief Marketing Officer to provide messaging for the communications strategy around the business disruption.	☐

Recovery Strategy # 1 – Loss of key or large number of people

Where a person with a key dependency is not available, or large number of persons will not be available, impacting on the ability for ACU to deliver Critical Business Functions.

9.	4-12 hrs	Employees to resume business operations in accordance with Critical Business Functions list.	☐
10.	12-24 hrs	Confirm that impacted employees have access to on-going EAP and trauma counselling services, if required.	☐
11.	Daily	Provide daily status report to CIRG on critical business capabilities.	☐
12.	1 week +	Provide information to CIRG to allow commencement of recruitment of permanent employees to replace key roles as needed.	☐
13.	1 week +	Assessment of potential insurance coverage.	☐
14.		Continue with Post Incident Actions.	☐

Recovery Strategy # 2 – Sustained Failure of IT and/or Communications Systems

Where IT or communications are not operational for a period of time that will impact ACU ability to continue delivering Critical Business Functions.

Step	Timing	Activity/Action/Task	☒
		Note: These timings are based on operational team members potentially requiring systems to maintain the campus operations. If the teams are not responding to incidents, timings may be longer.	
1.	2-4 hrs	If communications are affected, work with IT to divert phones.	☐
2.	2-4 hrs	If an extended downtime is anticipated (> 24 hours), determine requirement to activate IT Incident Management Process.	☐
3.	2-4 hrs	Commence detailed damage assessment of data and voice equipment.	☐
4.	2-4 hrs	Review Appendix D – Critical Business Functions list to assess all functions that might be impacted. *Detailed lists contained within appendices of the Business Recovery Plans.*	☐
5.	2-4 hrs	Establish a Recovery Plan for any disrupted functions.	☐
6.	2-4 hrs	Establish a communications strategy with MER to ensure key stakeholders are notified **in consultation with the Chief Marketing Officer**.	☐
7.	6-12 hrs	Provide relevant information to the CIRG to enable development of communications strategy for impacted stakeholders to notify of disruption, likely downtime and changes to services.	☐
8.	6-12 hrs	Contact any impacted third parties to advise of disruption and alternate procedures. This will include regulatory bodies.	☐

Recovery Strategy # 2 – Sustained Failure of IT and/or Communications Systems

Where IT or communications are not operational for a period of time that will impact ACU ability to continue delivering Critical Business Functions.

Step	Timing	Activity/Action/Task	☒
9.	6-12 hrs	Review Critical Business Functions list to assess all functions that might be impacted.	☐
10.	6-12 hrs	Work with IT in replacing IT equipment as determined by damage assessment.	☐
11.	6-12 hrs	Establish a Recovery Plan for any disrupted Critical Business Functions including: ○ Implementation of redundancies and work-around. ○ Requirement for relocation of essential employees. ○ Incident communications to affected parties. ○ Management of other business impacts caused by the failure of IT services.	☐
12.	Daily	Provide daily updates to affected stakeholders (in consultation with the Chief Marketing Officer).	☐
13.	Daily	Provide daily status report to CIRG on critical business capabilities.	☐
14.		Assessment of potential insurance coverage.	
15.		Continue with Post Incident Actions.	☐

Recovery Strategy # 3 – Denial of Access to Buildings

Where there is a denial of access to buildings for any reason, either short term or long term, that will result in ACU not being able to deliver Critical Business Functions.

Step	Timing	Activity/Action/Task	☒
		This may apply to a single premises or multiple premises, across the University.	
1.	0-2 hrs	Ensure people are safe, and account for your team/s.	☐
2.	0-2 hrs	If there has been substantial damage to the building, confirm that it has been secured and staff (and visitors) advised not to enter, including *Do Not Enter* signage at the entry points, and the building locked to ensure staff and visitors cannot enter.	☐
3.	0-2 hrs	Determine if there are any key risks that require containment e.g., chemicals, biological hazard etc.	☐
4.	0-2 hrs	If there has been substantial damage to the building, liaise with the Facilities team for them to commence a detailed damage assessment of the physical environment and equipment to determine extent of disruption to operations	☐

Recovery Strategy # 3 – Denial of Access to Buildings

Where there is a denial of access to buildings for any reason, either short term or long term, that will result in ACU not being able to deliver Critical Business Functions.

Step	Timing	Activity/Action/Task	☒
5.	0-2 hrs	If there has been other damage caused to the building, such as pests, water damage etc, confirm that the Facilities Team has organised relevant contractors to assess the building.	☐
6.	0-2 hrs	Determine likely downtime estimate. If extended downtime is estimated (greater than 24 hrs), initiate employee relocation strategies (alternate location or remote workplace). Determine requirement to activate other Recovery Strategies.	☐
7.	0-2 hrs	Determine if animals require relocations.	☐
8.	0-2 hrs	Liaise with the Chief Warden / Facilities Management or relevant team member to establish the disruption timeframe.	☐
9.	0-2 hrs	Work with IT to establish access to core IT systems for remote working.	☐
10.	0-2 hrs	Advise Facilities of areas needing to be secured.	☐
11.	0-2 hrs	Determine if any buildings require generator power.	☐
12.	2-4 hrs	Identify if there are personal belongings still on premises that may need obtaining.	☐
13.	2-4 hrs	Arrange for security measures as appropriate (e.g. security guards, additional security patrols, temporary CCTV cameras and alarms) at affected premises (if required).	☐
14.	2-4 hrs	Work with the CIRG to notify all key employees to commence relocation to alternate site or remote work locations.	☐
15.	6-12 hrs	Provide the CIRG with information to notify suppliers and key stakeholders of disruption, temporary location, and contact details.	☐
16.	6-12 hrs	Place signage outside office(s) / site(s) to advise of disruption and contact details.	☐
17.	6-12 hrs	Site manager to advise key contractors (e.g., cleaners, waste removal, supplies providers, etc.) and any other persons that use the site that the site is closed and not to enter.	☐
18.	6-12 hrs	Work with organisational units to review Critical Business Functions list to assess all functions that might be impacted.	☐
19.	6-12 hrs	Establish a recovery plan for any disrupted Critical Business Functions including: ○ Requirement for relocation of employees to alternate sites. ○ Availability of IT accesses for employees to work from alternate site and/or home. ○ Initial communications to employees, visitors and affected third parties. ○ Transportation requirements including management and relocation of significant assets to other sites.	☐

Recovery Strategy # 3 – Denial of Access to Buildings

Where there is a denial of access to buildings for any reason, either short term or long term, that will result in ACU not being able to deliver Critical Business Functions.

Step	Timing	Activity/Action/Task	☒
20.	6-12 hrs	Confirm work from home or arrangements for essential employees at alternate sites.	☐
21.	6-12 hrs	Organise transport for staff to either home or alternate premises if required.	☐
22.	12-24 hrs	Work with Properties and Facilities to assess available infrastructure as required.	☐
23.	12-24 hrs	Establish alternative work locations in line with pre-determined locations – refer to the Business Recovery Plans.	☐
24.	24-48 hrs	Review classes to be relocated and re-timetabled or moved online.	☐
25.	24-48 hrs	Employees to resume operations at alternate site / remote location as per Critical Business Functions list.	☐
26.	24-48 hrs	Contact third party service providers to arrange additional resources, as required.	☐
27.	24-48 hrs	Place order for replacement equipment.	☐
28.	48-72 hrs	If damaged site is accessible and deemed safe, employees may enter premises to retrieve critical documents, upon advice from the Business Recovery Leader following advice from the emergency services or Critical Incident Convener.	☐
29.	48-72 hrs	If necessary, employees to transport all equipment and documents to alternate site.	☐
30.	Daily	Provide daily status report to CIRG on critical business capabilities.	☐
31.		Assessment of potential insurance coverage.	
32.		Continue with Post Incident Actions.	

Recovery Strategy # 4 – Failure of Material / Critical Service Provider

Where a critical service provider is not able to deliver its services, resulting in inability for ACU to deliver its Critical Business Functions.

Step	Timing	Activity/Action/Task	☒
1.	0-2 hrs	Conduct detailed assessment of service interruption and identify impacted functions. Obtain downtime assessment from Service Provider.	☐
2.	2-4 hrs	Assess all Critical Business Functions and work-in-progress affected by loss and/or failure of material service provider.	☐

Recovery Strategy # 4 – Failure of Material / Critical Service Provider

Where a critical service provider is not able to deliver its services, resulting in inability for ACU to deliver its Critical Business Functions.

Step	Timing	Activity/Action/Task	☒
3.	2-4 hrs	Notify relevant stakeholders of the interruption **in consultation with the Chief Marketing Officer**.	☐
4.	2-4 hrs	Obtain recovery action plan from Service Provider detailing: ○ extent of disruption; ○ recovery Time Objectives for impacted functions; ○ workarounds to restore Critical Business Functions; and ○ Communication strategies.	☐
5.	2-4 hrs	Establish a recovery plan for any disrupted Critical Business Functions including: ○ conducting a stocktake of existing stock; ○ determining required stock levels to maintain Critical Business Functions; ○ implementation of interim measures and manual workarounds; ○ determining if the supplies are available at alternate campuses; ○ requirement to engage with an alternate provider or expert; ○ initial communication to staff and other impacted third parties; ○ management of other business impacts caused by the failure of services; ○ financial assessment; and ○ provide proposed recovery strategy to the Critical Incident Convener.	☐
6.	4-6 hrs	Determine availability of alternate service providers to assist with the recovery of Critical Business Functions, if required.	☐
7.	4-6 hrs	Confirm that the key stakeholders have been informed of business interruption.	☐
8.	6-12 hrs	If supply from an alternate location is unavailable, assess work-in-progress and employee requirements.	☐
9.	1 week +	Assessment of potential insurance coverage.	
10.	Ongoing	Liaise with service provider/s on a regular basis to keep updated of the situation and expected recovery timeframes.	☐
11.	Ongoing	Monitor implementation of the recovery plan and status of affected Critical Business Functions. Provide updates to the Business Recovery Lead.	☐
12.	Ongoing	Provide ongoing status reports to the CIRG on the situation and the likely impact on critical business capabilities.	☐

Recovery Strategy # 5 – Loss of Research

Where research will be significantly impacted during a disruption, resulting in a major or severe risk rating.

Step	Timing	Activity/Action/Task	☒
1.	0-2 hrs	Speak with Facilities to assess the safety requirements of impacted research material/resources.	☐
2.	0-2 hrs	Liaise with staff to transfer, relocate or lockdown at risk materials, in consultation with Facilities.	☐
3.	0-4 hrs	Liaise with impacted researcher to conduct a detailed assessment of impacted research.	☐
4.	2-4 hrs	Liaise with IT Support if loss of research was caused by an IT equipment failure.	☐
5.	6-12 hrs	Conduct briefing to CIRG.	☐
6.	6-12 hrs	Determine requirement to inform relevant third parties (investors, stakeholders) and external agencies (Police etc.) **in consultation with the Chief Marketing Officer**.	☐
7.	Daily	Provide daily status report to CIRG on the situation and the likely impact on critical business capabilities.	☐
8.		Assessment of potential insurance coverage	

Post Incident Actions

Step	Timing	Activity/Action/Task	☒
1.	24 hrs+	Complete task log.	☐
2.	24 hrs+	Develop a plan to enable an orderly switch-back of critical functions and employees from any alternate sites to primary site.	☐
3.	24 hrs+	Declare deactivation of the Business Continuity Plan for this event with approval of the Critical Incident Convener.	☐
4.	24 hrs+	In liaison with the CIRG, conduct post incident review involving key employees, other Business Areas and relevant stakeholders.	☐
5.	24 hrs+	Review BCP and amend accordingly if required.	☐
6.	2 weeks+	Lodgement of detailed insurance claim (if applicable).	

Phase 3: Implementing Business Resumption

The following checklist guides the steps required to return the organisation to pre-interruption status. The Business Recovery Lead will work with the organisational units and the Business Recovery Lead in implementing the actions noted within this checklist.

Step	Task	Done
1.	Continue referring to the list of Critical Business Functions to ensure restoration in conjunction with the longer-term resumption.	☐
2.	Deactivate staff members and resources, as necessary.	☐
3.	In conjunction with the CIRG and the Chief Marketing Officer, assist with developing communication messages for relevant stakeholders to update them on progress of business resumption.	☐
4.	Work with Facilities Management and the National Manager, Safety & Wellbeing, in relation to any injuries sustained during the incident or disruption. Ensure liaison is occurring with WorkSafe NSW, doctors and insurance companies to facilitate ongoing care of injured, and back to work plans.	☐
5.	Liaise with Privacy Coordinator regarding any notifications required.	☐
6.	Facilitate notification of disruption to Insurance companies.	☐
7.	Maintain a log of all steps taken after the disruption (time, location, action, delegations, work orders, invoices, etc).	☐
8.	Take photographs (or videotape) of damaged and undamaged facilities, infrastructure, etc.	☐
9.	Consult with business areas and contractors for initial estimate of the scope and cost of repairs.	☐
10.	Engage with the Properties and Facilities early in assessing damage.	
11.	Engage financial accountant to lodge a detailed insurance claim.	
12.	Identify internal and external resources to perform restoration activities.	☐
13.	When deemed safe, organise retrieval of any damaged and undamaged media and equipment from buildings to minimise loss.	☐
14.	Gain approval / source funding for required restoration or relocation of site.	☐
15.	Make plans for repairing the damage to buildings. Consider potential improvements to buildings as part of this process.	☐
16.	If repairs are not possible in the short term, determine the need to relocate to an alternate location. Work with Facilities Management.	☐
17.	Assess future Business Continuity management needs in the planning process.	☐
18.	Commence restoration or relocation of site(s) and buildings.	☐
19.	Dispose of damaged properties and equipment.	☐
20.	Complete restoration or relocation process.	☐
21.	Business Recovery Lead issue a deactivation notice via the Critical Incident Convener.	☐
22.	Resume normal business operations.	☐
23.	Advise key stakeholders that normal business operations have resumed.	☐

Appendices

Appendix A – Definitions

Definition	Description
Activation	The act of declaring that an organisation's incident management arrangements need to be put into effect to respond, recover and resume operations.
Alternate Site	A pre-established site held in readiness for the recovery and resumption of business operations in the event of a disaster to maintain the organisation's mission critical activities and objectives.
Business Continuity	The capability of the organisation to continue delivery of products or services within acceptable time frames at predefined capacity during a disruption.
Business Continuity Management	A holistic management program that identifies potential events that threaten an organisation and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, the environment, reputation, brand and value creating activities.
Business Continuity Plan (BCP)	Documented information that guides an organisation to respond to a disruption and resume, recover and restore the delivery of products and services consistent with its business continuity objectives.
Communications Plan	Provides sufficient information to enable the organisation to identify internal and external stakeholders, methods, and channels for communicating and formatted messaging to enable a response to a disruption.
Critical	A qualitative description used to emphasise the importance of a resource, process or function that must be available and operational constantly or at least at the earliest possible time after an incident, emergency or disaster has occurred.
Critical Incident Response Group (CIRG)	A trained group of people with defined roles and responsibilities, assigned to respond and manage an incident.
Critical Business Functions (CBF)	Vital functions, without which the organisation cannot effectively operate and as a result could suffer serious reputation, financial, legal, or other damages or penalties.
Critical Supplier	Provider of products / services whose loss would quickly disrupt the organisation's critical activities.
Disaster Recovery Plan	The document outlining the process for recovering the business IT systems.
Disruption	An event that interrupts normal business functions, operations, or processes, whether anticipated (e.g. extreme weather, political unrest) or unanticipated (e.g., blackout, terror attack, earthquake).
Recovery Strategy	An approach used by an organisation to ensure its recovery and continuity in the face of a disaster or other major incident or business disruption.
Recovery Support Procedure	Detailed procedures to assist with the effective implementation of a Recovery Strategy based on defined disruption scenarios.
Recovery Time Objective (RTO)	The period of time following an incident within which a product or service must be resumed, or activity must be resumed, or resources must be recovered.
Resources	All assets, people, skills, information, technology (including plant and equipment), premises, and supplies and information (whether electronic or not) that an organisation has to have available to use, when needed, in order to operate and meet its objective.

Appendix B – Information Collection Form

The following may be used by the Critical Incident Convener or Business Recovery Lead when receiving information about an incident or potential disruption. This collection form is focused on business continuity however has a few questions around emergency management in the event immediate actions may need prompting.

Questions to ask
(these are a series of questions you may wish to ask to gather information – the list is not exhaustive, and the person notifying of the event may not have all the answers)

- What has happened?
- Where did it happen?
- Who is involved?
- Any casualties?
- Is everyone safe?
- Has emergency management been initiated?
- What is the business disruption?
    - Loss of key person or large group of people
    - Denial of access to building
    - Sustained failure of IT and/or communications systems
    - Failure of material / critical service provider
- Is the situation contained or still escalating?
- What is the estimated timeframe of the disruption?
- Is media involved?
- What action has been taken so far?
- What assistance is required?

Events details			
Event date		Event time	
Event overview		Event location	
Name of person advising / notifying of the event		Contact number of person advising	
Event statement assessment			
Event disruption	☐ Loss of key person ☐ Denial of access to building ☐ Sustained failure of IT and/or communications systems ☐ Failure of material / critical service provider		
Decision maker name		Decision maker contact number	
Other notes			

Appendix C – Contact Details

Contact details can be located via this link and all members of the CIRG should save the contacts so they can be available offline in the event of a network outage or loss of connectivity.

Appendix D – Critical Business Functions

To be updated following review of BIAs under new structure

Utilise this list to assess the functions impacted, and to recover Critical Business Functions within Recovery Time Objectives (RTO's). The below listing contains only those functions **up to 24 hours**. Refer to the Business Recovery Plans for detailed listings per Business Area.

The Maximum Allowable Outage (MAO) and Recovery Time Objectives (RTO) were determined from the Business Impact Analysis. The BIAs focus on identifying the Critical Business Functions along with the timeframe (MAO) at which point the impact or the consequence of not being able to deliver the critical functions would move beyond a moderate impact according to the risk rating matrix.

Tier 1 Critical Business Functions (≤ 24 hours RTO)

Ref.	Critical Business Function	Portfolio	Organisational Unit	MAO	RTO

Appendix E – Impact and issues assessment

The Business Recovery Lead should use the 'Financial' and 'Operational' component of the *Impact and Issues Assessment Tool* to determine the impact to ACU resulting from business disruption, with a focus on formulating strategies to recover the business operations.

1. Operations			
To what extent is the event likely to impact the delivery of operational services by ACU?			
Impacted Operational Business Area	**Impact**	**Mitigating Action**	**Owner of Action**

2. Financial				
To what extent is the event likely to result in financial losses or impact on ACU?				
Cause of Financial Impact	**Assessed cost of Impact**	**Within budget? (Yes/No)**	**Mitigating Action**	**Owner of Action**
Significant budgetary realignment				
Financial management				

Appendix F – Critical Documents Register

To be updated following review of Critical Incident Management Procedure and associated documents

The following table identifies critical documents and where to locate them.

Document Name	Description	Storage Location	Responsibility
[insert]	[insert]	[insert]	[insert]

Appendix G – Briefing Template

This briefing template aids information exchange.

Briefing by:		Briefing to:	
Date:		**Time:**	**Version:**

Situation *What is currently happening?*			
Impacts *What are the primary and secondary impacts? Link this from the impact assessment*	Primary: Secondary:	▪ Human ▪ Reputational ▪ Financial ▪ Operational	▪ Legal ▪ Environmental ▪ Strategic
Risks to ACU *What is likely to happen, or could happen?*			
Objectives & Execution *What does the CIRG need to achieve prior to the next meeting?* *How will we achieve the objectives?* *Are any additional resources required?*			
Administration *How often will the CIRG meet?* *What are the shift arrangements?* *What welfare arrangements are needed?*			
Command & Communications *Who is the strategic Emergency Services contact?* *Attach the comms plan*			

Appendix H – Task Log

Complete the following to record your key actions.

Time/Date	Action	Tasked to	☒
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☒
			☐
			☐
			☐