Business Continuity Management Framework

Section 1 - Introduction

(1) Business Continuity Management (BCM) is a University of Newcastle (University) wide capability that supports organisational resilience by enabling the University to sustain delivery of critical services during and following a disruption.

(2) BCM focuses on understanding the impact of disruption to the University's teaching, research and operational activities, and establishing arrangements to maintain or restore those services within acceptable timeframes.

(3) Disruptions may arise from a range of events, including natural disasters, pandemics, infrastructure failure, loss of systems, cyber incidents, and other incidents that may impact the University's ability to operate.

(4) The safety of students, staff, contractors and visitors remains the University's first priority. Following this, BCM supports the continuity and recovery of critical services.

Section 2 - Audience

(5) This Framework applies to all of the University and its controlled entities.

Section 3 - Purpose

(6) This Framework provides the structure, processes and tools required to implement Business Continuity Management across the University.

(7) It supports the Business Continuity Management Policy and establishes a consistent approach to identifying critical services, assessing disruption impacts, and developing continuity arrangements.

Section 4 - Scope

(8) This policy applies to all areas and locations of the University and its controlled entities, and to all activities that support the continuity of critical services in the event of disruption, including dependencies on people, systems, facilities and third parties and services provided by Digital Technology Solutions and external partners.

Section 5 - Business Continuity Management Life Cycle

(9) The University applies a structured lifecycle to business continuity management comprising:

a. Identify – determine critical services and key dependencies;
b. Analyse – assess likely impacts of disruption;

c. Plan – develop Business Continuity Plans and strategies;
d. Activation and response – implement continuity arrangements to sustain or restore critical services during a disruption;
e. Validate – test and exercise plans and arrangements; and
f. Improve – implement lessons learned and enhance capability.

Section 6 - Identify

(10) Business continuity management begins with the identification of critical services and the resources, dependencies and arrangements required to support their delivery.

(11) Critical services may rely on people, facilities, information, technology systems, suppliers, third-party providers and other supporting resources.

(12) Disruption-related risks are identified and managed in accordance with the University's Risk Management Framework.

Section 7 - Analyse

(13) Business impact assessments (BIAs) are the foundation of the BCM program and are used to identify critical services and assess the impact of disruption.

(14) BIAs consider dependencies including people, infrastructure, systems, suppliers, third-parties, and information.

(15) Risk Services will coordinate the University's Business Impact Assessment program and establish the methodology and supporting processes. Colleges, Divisions, business units and controlled entities are responsible for participating in the assessment of functions within their areas of responsibility and maintaining relevant business continuity information.

(16) BIAs should be reviewed periodically to ensure they remain current and reflect changes to critical services, dependencies and operating environments. Reviews may be triggered by significant organisational, operational, technology or service delivery changes, following a disruptive incident, or as part of scheduled BCM activities.

(17) BIAs define recovery priorities, including maximum acceptable outage and recovery time objectives, which inform continuity planning and system recovery priorities.

Section 8 - Plan

(18) Business Continuity Plans (BCPs) are informed by BIAs and document the arrangements required to sustain or restore critical services during and following a disruption.

(19) Leaders of Colleges, Divisions, business units and controlled entities are responsible for developing and maintain BCPs.

(20) BCPs should include:

a. critical services and priorities;
b. activation and escalation arrangements;
c. continuity strategies and workarounds;
d. roles and responsibilities;

e. communication requirements;
f. key internal and external dependencies; and
g. recovery arrangements.

(21) BCPs should be maintained in a manner that supports accessibility during disruption, including consideration of scenarios where normal ICT systems may be unavailable.

(22) Continuity strategies should be proportionate to the criticality of the service and consider the arrangements necessary to sustain or restore service delivery during a disruption.

(23) Depending on the nature of the service, continuity strategies may address matters including:

a. personnel and workforce availability;
b. facilities and alternate work locations;
c. information, records and data recovery;
d. technology systems and supporting infrastructure;
e. suppliers, contractors and their-party providers;
f. communications and stakeholder engagement;
g. legislative, regulatory or contractual obligations; and
h. health, safety and wellbeing considerations.

(24) BCM operates in conjunction with:

a. the Incident Management Framework, which governs operational response to incidents;
b. the Crisis Management Plan, which governs coordination and decision-making during critical incidents; and
c. Information and Communications Technology (ICT) Disaster Recovery arrangements, managed by Digital Technology Solutions.

Section 9 - Activation and Response

(25) BCPs may be activated where a disruption impacts, or is likely to impact, the delivery of critical services.

(26) During a disruption, BCPs support the continuation or restoration of critical services while incident response activities are managed in accordance with the University's Incident Management Framework and, where required, the Crisis Management Plan.

(27) Activation may occur:

a. as directed through the University's incident or crisis management arrangements where broader coordination is required; or
b. at a local level, by the responsible business area, with notification to Risk Services.

(28) BCPs should remain active until critical services have been restored to an acceptable level or alternative arrangements have been established.

Section 10 - Validate

(29) Risk Services coordinates training and exercises to validate and develop business continuity capability.

(30) Colleges, divisions, business units and controlled entities must participate in testing and maintain awareness of their roles and responsibilities.

(31) Validation activities may include exercises, walkthroughs, reviews and activation of continuity arrangements.

Section 11 - Improve

(32) Post-incident reviews and exercise outcomes are used to identify lessons learned and opportunities for improvement.

(33) BCM capability will be progressively developed in alignment with the University's BCM Roadmap, under the oversight of the Chief Operating Officer.

(34) As capability matures, a structured review approach will be introduced for priority services, with review frequency determined based on service criticality and risk.

(35) Business Continuity Plans and associated artefacts will be reviewed periodically to ensure they remain current and may require updating following:

a. significant organisational change;
b. changes to critical services or dependencies;
c. technology or infrastructure changes;
d. outcomes from exercises or testing activities; or
e. a disruptive incident.

(36) Continuous improvement will be informed by BIAs, testing, exercises and post-incident reviews.

Section 12 - Related Documents

(37) Business Continuity Management Policy

(38) Incident Management Framework

(39) Crisis Management Plan

(40) Risk Management Framework

Status and Details

Status	Current
Effective Date	11th November 2026
Review Date	11th November 2027
Approval Authority	Chief Operating Officer
Approval Date	16th October 2026
Expiry Date	Not Applicable
Responsible Executive	Morven Cameron Chief Operating Officer
Enquiries Contact	Virginia McKay Director, Risk Services Risk Services

Glossary Terms and Definitions

"University" - The University of Newcastle, a body corporate established under sections 4 and 5 of the University of Newcastle Act 1989.

"Risk" - Effect of uncertainty on objectives. Note: An effect is a deviation from the expected, whether it is positive and/or negative.

"Controlled entity" - Has the same meaning as in section 16A of the University of Newcastle Act 1989.

"Student" - A person formally enrolled in a course or active in a program offered by the University or affiliated entity.

"Research" - As defined in the Australian Code for the Responsible Conduct of Research, or any replacing Code or document.

"Staff" - Means a person who was at the relevant time employed by the University and includes professional and academic staff of the University, by contract or ongoing, as well as conjoint staff but does not include visitors to the University.

"College" - An organisational unit established within the University by the Council.

This document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to the Policy Library for the latest version.