Business Continuity Management Framework

Section 1 - Introduction

(1) Business Continuity Management (BCM) is a University wide activity that identifies threats to the University of Newcastle (University) and the impact to operations should those threats eventuate. BCM provides a framework for building organisational resilience, supporting the capability to effectively respond to incidents that cause business disruption.

(2) Business Continuity (BC) encompasses planning and preparation to ensure the University can continue to operate, or recover to an operational state, in the event of a business disruption within a reasonable timeframe. BC focuses on the resilience of people, property, processes, systems and providers as well as the availability and integrity of information.

(3) Disruption-related risks are infrequent, high consequence events that impact people and operations, and are not resolved through routine management. Disruption-related risks include physical and non-physical events such as natural disasters, pandemics, significant loss of utilities, infrastructure, systems, accidents and incidents that threaten the University, students and staff.

(4) The first priority in a disruptive incident is the immediate and ongoing safety of students, staff, contractors and visitors. Following this is availability of critical people, systems and processes to revert to normal business or implement a new mode of operation as soon as appropriate.

(5) Past incident recovery strategies are detailed in the University's Emergency Management Procedures and Business Continuity Plans.

Section 2 - Audience

(6) This Framework applies to the University in the entirety, including all controlled entities.

Section 3 - Background

(7) Business Continuity Management is an application of risk management, an integral component of sound corporate governance, and an important aspect of emergency preparedness and operational resilience.

(8) An effective Business Continuity Management Framework will assist the University Council, Risk Committee and Vice-Chancellor in obtaining reasonable assurance that:

a. disruption-related risks are clearly identified and managed appropriately, with consideration to the Council's risk appetite.
b. the objectives of business continuity management are met, including maintaining health and safety, minimising reputational damage, ensuring effective communication between stakeholders, protecting vital and intellectual assets, expediting recovery after a disruptive incident, and reducing vulnerability to future incidents.

(9) This Framework provides the foundations and organisational arrangements for an integrated, risk based and effectively managed business continuity program. It is designed to provide direction and support to the University and its key personnel in implementing a business continuity program, including the development and maintenance of robust, flexible and well exercised plans.

(10) The University's Business Continuity Management Framework is based on the preparation of:

a. Business Impact Assessments (BIA);
b. Business Continuity Plans (BCP);
c. disaster recovery planning for critical infrastructure and resources;
d. communications and media liaison strategies; and
e. crisis management, recovery, and emergency planning.

(11) The Business Continuity Management Policy and Framework have been prepared based on the International Standard as adopted by Standards Australia - AS/NZS ISO 22301:2012, and the Business Continuity Institute’s Good Practice Guidelines (GPG) 2018 Edition.

Section 4 - Principles

(12) The University's Business Continuity Management Framework supports the following key principles, as the key qualities to effective business continuity management:

a. business continuity management is part of decision making and is undertaken in a systematic, structured and timely manner, contributing to efficiency and comparability.
b. business continuity management is tailored with the risk and emergency management arrangements to ensure appropriate response and recovery plans are in place.
c. appropriate business continuity workarounds and strategies are implemented to allow for continuing provision of critical processes.
d. mechanisms for notifications, alerts and escalation of disruptive incidents are provided.
e. business continuity and emergency management arrangements are exercised and tested regularly to ensure plans remain up-to-date and effective.
f. Business Continuity Plans, procedures, strategies, workarounds, and associated documents are reviewed and updated regularly.
g. education and training is provided to staff who hold business continuity roles and responsibilities.
h. resilience and organisational capacity is built through the application of robust and consistent business continuity practices.
i. Business Continuity Management is a system of continual improvement.

Section 5 - Approach to Business Continuity Management

(13) The Business Continuity Management Policy confirms the University's commitment to business continuity management. It sets out the approach to enhancing the University's business continuity management capability, maturity and ensuring continual improvement.

(14) Business continuity management should be performed continually and is not simply about responding to events. The University supports a risk based business continuity program which encompasses the Plan-Do-Check-Act (PDCA)

model. This model embraces planning, establishing, implementing, operating, monitoring, reviewing and continually improving the effectiveness of the University's business continuity management program (refer ISO 22301:2012(E) PDCA Model).

(15) Business continuity planning is a key function within the University's business continuity program. It is a continual process of identifying hazards and vulnerabilities, the likelihood of disruption, potential consequences on time-sensitive objectives and strategic success, existing control effectiveness, and strategies to improve performance and efficiency.

(16) Business Continuity Plans for the University's critical processes are integrated with emergency management arrangements. These plans assist in the identification of IT resources required to support the delivery of critical business processes, which may be used to inform the development of Information Technology Disaster Recovery Plans (ITDRP).

Section 6 - Disruption-Related Risk Assessment

(17) Committing to the University's risk-based program increases awareness of disruption-related risks, continuity planning, and response management, and supports staff to effectively work around a business disruption until full functionality is restored or a new mode of operation implemented.

(18) Business processes are risk-assessed for their criticality or value to the University's mission using a consistent, common criteria and relevant metrics.

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

Section 7 - Business Impact Analysis / Assessment (BIA)

(20) Risk assessment and business impact analysis are essential steps when creating a Business Continuity Plan. Where risk assessment identifies and assesses potential hazards, a business impact analysis focuses on the consequences to critical processes during a disruptive incident.

(21) The business impact analysis considers the functions, people, processes, activities, equipment, infrastructure, systems, resources, information, dependencies, and the extent of business disruption over time.

(22) College / Divisions are required to maintain a business impact analysis and Business Continuity Plan for the critical processes in their area that support the University's critical objectives. These objectives are:

a. manage student admissions (domestic and international);
b. manage student enrolments (domestic and international);
c. receive and process student enrolment fees;
d. manage and facilitate courses;
e. manage and facilitate examinations (paper and electronic);
f. maintain critical research;
g. pay staff;
h. pay creditors;
i. ensure census date arrangements are available;
j. approve and submit research grant applications; and

k. receive and process research grant revenue.

(23) As part of the business impact analysis, College / Divisions are required to identify seasonal variations, legal or compliance obligations, third party suppliers, IT systems, resources, dependencies and consequences of not performing the critical process. In addition, College / Divisions are required to define the maximum allowable outage (MAO), recovery time objective (RTO) and recovery point objective (RPO) for each critical process.

(24) Based on the outputs from the business impact analysis, College / Divisions are required to determine appropriate business continuity strategies to be implemented for resuming and recovering critical processes during and following a disruptive incident. These strategies form an essential component of Business Continuity Plans.

Section 8 - Business Continuity Strategies, Plans and Procedures

(25) The University's strategies and decisions are based on the assumption that assets, people, systems and key processes will be available and delivered as normal.

(26) When a disruption occurs there is usually little time to assess which impacted business processes and resources are most critical. Crucial decisions are required quickly to divert resources and ensure sustainability of critical processes.

(27) College / Divisions responsible for critical processes are required to determine an appropriate business continuity strategy and timeframe, specifically for:

a. protection, stabilisation and continuation;
b. resumption and recovery;
c. dependencies and supporting resources; and
d. mitigation, response to, and management of a disruptive incident.

(28) In addition, College / Divisions are required to identify and determine the requirements to implement appropriate strategies, including but not limited to:

a. people;
b. buildings, work environment and associated utilities;
c. facilities, equipment and consumables;
d. information, data and communication technology systems;
e. transportation;
f. finance;
g. partners and suppliers; and
h. communications.

(29) Some business continuity strategies can be applied across all Colleges, Schools, Divisions and Units, however some are unique to individual teams. Each critical process should have its own continuity strategy, which can be invoked individually or en masse as required.

Colleges, Schools, Divisions and Units Business Continuity Plans

(30) The business continuity strategies and arrangements for a College, School, Division and Unit are documented in the Business Continuity Plan. The Business Continuity Plan informs the reader of the priority processes, equipment,

systems and infrastructure required should an incident occur, and provides a guide for relocation, restoration and recovery.

(31) A Business Continuity Plan consists of an action plan and the steps necessary to relocate, restore and recover during and after a disruptive incident. It is not intended to provide full procedural information on undertaking the underlying activities themselves, but needs to contain adequate detail to assist the reader to complete them correctly. A Business Continuity Plan should define:

a. critical processes to be sustained;
b. activation criteria and procedures;
c. immediate steps and implementation procedures;
d. key assets, systems and resources required to support critical processes;
e. internal and external communication requirements and procedures;
f. roles, responsibilities and back-up personnel;
g. internal and external dependencies and interactions;
h. vital records and storage details to support business resumption;
i. continuity strategies;
j. maximum acceptable outage;
k. recovery time objectives and recovery point objectives;
l. alternate accommodation arrangements; and
m. notification and escalation procedures.

(32) Alternate strategies may be appropriate during the recovery phase and should be documented in individual Business Continuity Plans.

(33) To assist College / Divisions, the University's Business Continuity Plan includes examples of the following scenarios, in which College / Divisions are required to document the initial (manual) work-around, longer term solution, and recovery for:

a. critical impact on staff (inability to maintain processes due to insufficient staff numbers);
b. denial of access to building(s), floors and precinct (assets inside the building are not lost but cannot be accessed);
c. loss of workplace (permanent loss of non-electronic records, research materials, equipment, inability to undertake lectures);
d. loss of IT systems (inability to maintain processes or use equipment due to failure of key IT systems);
e. loss of utilities (temporary loss of electricity, gas, water etc.); and
f. University-wide incident (incident impact is across multiple Colleges, Schools, Divisions or Units and/or impacting multiple priorities).

(34) Recovery of some activities will be coordinated at a University level, however, in some circumstances the responsibility for recovery activities is delegated to the individual College, School, Division or Unit.

(35) In the event of a business disruption, staff must understand what is expected of them and should regularly rehearse their roles and test the Business Continuity Plan’s practicality, competency and assumptions, specifically around access to resources.

(36) The University's Business Continuity Plan template is prepared and maintained by the Risk Unit.

University Emergency and Business Continuity Management Plans, Procedures and Strategies

(37) In addition to individual Business Continuity Plans, the University's overarching Emergency Management and Business Continuity Plan is developed and maintained by the Risk Unit. The Risk Unit, in consultation with the University's Critical Incident Team and Emergency Planning Committee, maintain up-to-date, well tested plans and procedures (including necessary arrangements) for:

a. internal and external warning and communication protocols (including templates);
b. immediate steps to be taken during a disruption;
c. impact of events that could potentially disrupt operations;
d. flexible response to unanticipated threats, changing internal and external conditions;
e. reasonable assumptions and interdependencies;
f. appropriate mitigation strategies for implementation to minimise consequences;
g. identification of appropriate impact thresholds that justify initiation of a formal response;
h. assessment of the nature and extent of the incident and its potential impact;
i. appropriate processes and procedures for activation, operation, coordination and communication, including with interested parties, authorities and the media;
j. procedures to restore and return activities from the temporary measures to normal business as usual, following an incident; and
k. ensuring resources are available to support the processes and procedures, in order to minimise the impact.

Section 9 - Emergency Communications

(38) The University has an overlapping Emergency Communication strategy to provide early warning, real time messaging in the event of an emergency situation. The combination of one or more mediums of communication ensures emergency messages reach a many people as possible in a timely manner.

Section 10 - Activating Emergency Management and Business Continuity Plans

(39) Subsequent to notification of a critical incident, the Critical Incident Team is required to assess information, potential impact and determine whether normal business operations can resume. In the event normal operations cannot resume, it is the role of the Critical Incident Team to declare a critical incident and initiate partial or full activation of the appropriate plans.

(40) Where a critical incident requires a University wide response, notification to activate Business Continuity Plans is authorised and communicated by the Critical Incident Team.

(41) In the event that a Business Continuity Plan requires activation without notification from the Critical Incident Team, the Risk Unit is to be contacted and consideration taken for any other College, School, Division or Units that might be impacted.

Section 11 - Resuming Normal Operations (Stand-

Down)

(42) The Critical Incident Director will determine when the event is over and will advise staff, students and key stakeholders when it is appropriate to stand-down the CIT and resume normal operations.

Section 12 - Post Incident Review

(43) In the event a Business Continuity Plan is activated, a post incident review (PIR) will be held in consultation with the Risk Unit to consolidate lessons learned and develop, address and rectify opportunities for improvement.

(44) Following a significant critical incident, test or activation of a Business Continuity Plan, the Risk Unit will provide the Risk Committee with a post-incident report detailing the event/test, actions and decisions taken, any discrepancies, non-conformities and follow up actions.

Section 13 - Training and Testing

(45) The Risk Unit, in consultation with the Critical Incident Team and Emergency Planning Committee, maintain and regularly facilitate training and exercises incorporating procedures to:

a. detect a disruptive incident;
b. monitor an event;
c. assign roles and responsibilities;
d. manage internal communication within the University;
e. receive, document and respond to communication from interested parties, national or regional risk advisory systems or equivalent (e.g. Australian national security)
f. ensure availability of the means of communication during an event;
g. facilitate structured communication with external emergency responders;
h. respond to multiple organisations and personal;
i. record vital information about the event, actions taken and decisions made; and
j. provide induction training to new Critical Incident Team members, alternates, supporting roles and supporting teams

(46) At the discretion of the University, reviews will be undertaken at planned intervals from time to time to validate business continuity capabilities of key suppliers.

Section 14 - Key Roles and Responsibilities

(47) The following stakeholders play an important role with specific responsibilities:

Role	Business Continuity Management Framework Responsibility
University Council	The University Council and its Committees have responsibility under the University of Newcastle Act 1989 No 68 for overseeing risk, management and risk assessment activities across the University, including oversight of business continuity management.
Risk Committee	By delegation of the Council, the Risk Committee is responsible for: - Ensuring that the University embeds and maintains adequate business continuity management processes, culture and reporting mechanisms.
The Vice-Chancellor	Overall executive accountability for the University's business continuity capability and overall executive responsibility for the University's critical incident response.

Role	Business Continuity Management Framework Responsibility
College / Divisions	- Ensuring that business continuity management is integrated as an operational discipline that is appropriate supported and a suitable culture is promoted. - Attend scheduled tests relevant to their unit (Refer to the University's Testing and Review Schedule).
Critical Incident Team (CIT) (Refer Critical Incident Team and Emergency Planning Committee Membership)	- Responsible for the coordination and management of the response to a disruptive incident, including delegated authority to make decisions, direct staff and students, communicate with key stakeholders including the media and authorise expenditure. - Required to prioritise dealing with the event over other business tasks. - Attend scheduled tests where appropriate (Refer Testing and Review Schedule).
Emergency Planning Committee (Refer Critical Incident Team and Emergency Planning Committee Membership)	- Oversee the development, implementation and maintenance of the University's emergency planning, critical incident and business continuity management program.
University Secretary	- Coordinate the Business Continuity Framework and support the University in achieving appropriate capabilities, culture and maturity. - Ensure the Business Continuity Management Framework addresses the relevant strategic and operational risks. - Coordinate the development and review of business continuity management strategies, including Emergency Management Plans, Critical Incident Plans, Business Impact Assessments and Business Continuity Plans. - Report to the Vice-Chancellor and Risk Committee on the compliance of the Business Continuity Management Policy and Framework. - Ensure the Critical Incident Team is compromised of suitably skilled and experienced staff, including identification of appropriate alternates for each member. - Maintain the University's Critical Incident and Emergency Management Plans and associated training materials. - Facilitate the post incident review (PIR) process.
Risk Manager and Business Continuity Officer	- Develop the University's Framework, Policy, methodology and tools to enable business continuity management implementation across the University. - Provide central coordination, operational support, monitoring and reporting of all University business continuity management initiatives. - Facilitate and assist in the development and review of business continuity management strategies, including Emergency Management Plans, Critical Incident Plans, Business Impact Assessments and Business Continuity Plans. - Assist the Critical Incident Team to achieve their roles and responsibilities. - Support the maintenance of the University's Critical Incident and Emergency Management Plans and associated training materials. - Monitor and report compliance with the Policy and Framework to the University Secretary. - Facilitate training and awareness initiatives across the University. - Liaise with College, School, Division and Units to share relevant information on emergency management, critical incident and business continuity management. - Support the post incident review (PIR) process.

Section 15 - Review and Maintenance

(48) This Framework and the effectiveness of the business continuity management program will be reviewed by the College, School, Division and Unit in conjunction with the Risk Unit, at least annually or following any major operational or system changes that will have a material impact on the recovery strategy of the College, School, Division and Unit.

Section 16 - Appendices

(49) ISO 22301:2012(E) PDCA Model

(50) Critical Incident Team and Emergency Planning Committee Membership

(51) University Testing and Review Schedule

(52) Business Continuity Management Terms and Definitions

Status and Details

Status	Current
Effective Date	22nd January 2019
Review Date	31st December 2024
Approval Authority	Risk Committee
Approval Date	21st November 2018
Expiry Date	Not Applicable
Responsible Executive	Dianne Allen University Secretary dianne.allen@newcastle.edu.au
Enquiries Contact	Dianne Allen University Secretary dianne.allen@newcastle.edu.au Governance and Assurance 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.

"Risk management" - The co-ordination of activities to optimise the management of potential opportunities and reduce the consequence or impact of adverse effects or events.

"Risk appetite" - An organisation's approach to assess and eventually pursue, retain, take or turn away from risk.

"Risk assessment" - The overall process of risk identification, risk analysis, and risk evaluation.

"Asset" - Any tangible or intangible item (or group of items) that the University owns or has a legal or other right to control and exploit to obtain financial or other economic benefits.

"Census date" - The date in each term on which a student / candidate enrolled in a course is deemed to be financially liable for the course.

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

"School" - An organisational unit forming part of a College or Division, responsible for offering a particular course.

"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.