Business Continuity Management Framework

June 2017

University Operations

Risk, Assurance and Compliance

Campus and Collegiate Life Services | Campus Development | Chief Operating Officer
Health and Safety Compliance | Information Technology Services | Project Management
Property Services | Student Services | Sustainability

UNIVERSITY of OTAGO
Te Whare Wānanga o Otāgo
NEW ZEALAND
SAPERE AUDE

University of Otago | PO Box 56 | Dunedin 9054 | New Zealand

Enable | Engage | Experience

Document Control

Document ID: Put: \root directory \path here

Version No.	Date	Revision Details	Author	Endorsed	Approved
1.0	21 June 2017	Draft for consultation	M. Cartwright		
1.1	10 Ocotber 2017	Final version following consultation	M. Cartwright	S.Willis	Uni. Council

ACKNOWLEDGEMENTS

The Office of Audit, Risk and Assurance acknowledge those who created and implemented the existing Business Continuity Policy, associated processes, and tools at the University of Otago. These have created the foundation and context of this framework.

Further, the following resource documents have been relied on for development of this framework:

- Societal security – Business Continuity Management Systems – Requirements, ISO 22301:2012
- Tucker, E (2015). "Business Continuity from Preparedness to Recovery – A Standards-Based Approach". London. Elsevier.
- Risk management – Principles and guidelines, ISO AS/NZS 31000:2009

CONTENTS

Acknowledgement

Establishing the Business Continuity Management Framework

Implementation and Operation of the Business Continuity Management Framework

Monitoring and Improving the Business Continuity Management Framework

Glossary of Terms

Appendices

BUSINESS CONTINUITY MANAGEMENT FRAMEWORK

1. PURPOSE

The purpose of the Business Continuity Management Framework is to improve the University's capacity to withstand the negative impact of an incident whilst at the same time maintain critical academic, research, and business activities.

The framework provides management with a process to identify potential threats to the University and the impacts to critical functions that those threats, if they eventuated, could cause. It outlines the activities for responding to those threats in a manner that safeguards the interests of key stakeholders, reputation, and the services the University provides to students.

The framework is based on the International Standard 'Societal Security – Business Continuity Management Systems ISO 22301:2012 (BCMS).

Key elements of the framework are summarised in the following diagram:

The Business Continuity Management Framework

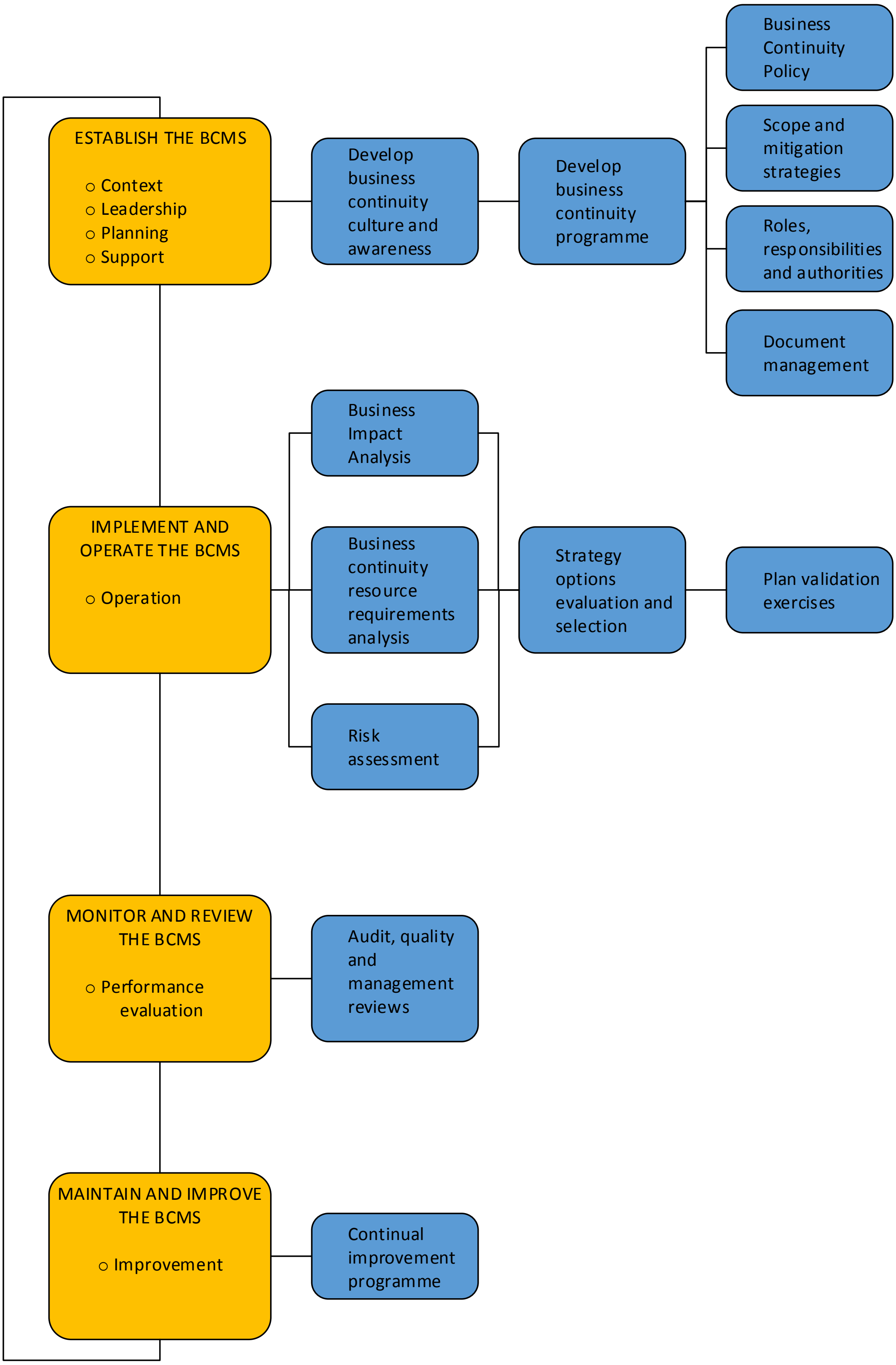
ESTABLISH THE BCMS
○ Context
○ Leadership
○ Planning
○ Support
Develop business continuity culture and awareness
Develop business continuity programme
Business Continuity Policy
Scope and mitigation strategies
Roles, responsibilities and authorities
Document management
IMPLEMENT AND OPERATE THE BCMS
○ Operation
Business Impact Analysis
Business continuity resource requirements analysis
Risk assessment
Strategy options evaluation and selection
Plan validation exercises
MONITOR AND REVIEW THE BCMS
○ Performance evaluation
Audit, quality and management reviews
MAINTAIN AND IMPROVE THE BCMS
○ Improvement
Continual improvement programme

Figure 1: University of Otago – Business Continuity Management Framework (ISO 22301:2012)

2. SCOPE

This framework applies to all areas of the University's business including its academic, research, administrative, support services, residential activities and commercial activities. It also applies to outsourced activities that support University operations and services.

Controlled entities of the University are responsible for their own business continuity management activities and provide reports on the status of those activities to the University's Audit & Risk Committee annually and on the request of the Committee.

Business continuity planning will initially be campus-based and focus on critical functions that support the delivery key services, giving due regard and priority to the health, safety, and well-being of staff, students, and the wider community. Key areas of operations will be introduced to the framework and associated planning activities using a staged implementation approach. The framework will then be extended to other areas of the University's business as the program matures.

3. BENEFITS

The Business Continuity Management Framework, Business Continuity Policy and associated planning activities ensure the University is able to operate at optimal, predefined levels of service in the event of a major disruption. The Business Continuity Management Framework:

- Ensures that procedures, from the initial business response to recovery and full functionality, are aligned and well understood.
- Clearly defines business continuity roles and responsibilities.
- Outlines the steps required to develop workforce resilience capability and competencies through plans, skills training, and plan validation exercises.
- Identifies the equipment and resources needed to recover and maintain critical services.
- Protects the University reputation/brand.
- Provides the means to identify and engage with key suppliers and contractors regarding business continuity.
- Supports the achievement of strategic and operational objectives.
- Supports compliance with regulatory obligations.
- Mitigates risks to operations, health and safety, property damage, and loss.
- Provides clarity in respect of the overlapping (and separate) duties associated with emergency management planning.

4. RISK GOVERNANCE

Risk governance refers to the culture and arrangements developed by the University to manage the risk to its mission and strategic objectives. It includes leadership, accountabilities, and oversight and is an essential part of the University's overall governance responsibilities.

The Business Continuity Framework is one element of the University's approach to mitigating risk - in this instance, disruption-related risk. The framework provides assurances that responses to disruptions are considered, co-ordinated, comply with regulatory requirements and meet the expectations of all stakeholders, particularly as it relates to the health, safety and well-being of staff, students, and the wider community.

Related Continuity Frameworks and Plans

There are a number of key frameworks and activities which form an important part of the University's overall business continuity capability. They include:

- Emergency Management Plan.
- Disaster Recovery Plan.
- Information Security Policy Framework (draft).
- Risk Management Framework.

Further information on the operation of these frameworks can be found in the Policy Library on the University website.

Sustainability

The staff responsible for the business resilience activities promoted by this framework are encouraged to consider the environment and the sustainability objectives of the University, as described in our Sustainability Strategic Framework: 2017-2021. Linking resilience efforts with our sustainability agenda may require some innovation but will result in better overall outcomes for the University and the wider community. Support and advice on methods for reducing the impact on our environment is available from the Office of Sustainability.

Business Continuity Policy

The Business Continuity Policy is a high level document that outlines the purpose, objectives, and governance arrangements for managing the business continuity programme. It is closely aligned with the Risk Management Policy and details the business continuity roles and responsibilities of staff. A copy of the Business Continuity Policy is located in the Policy Library on the University's website.

ESTABLISHING THE BUSINESS CONTINUITY MANAGEMENT FRAMEWORK

The steps involved in the development of the business continuity management framework and associated business continuity plans are summarised in the following table:

Process Step	Step Summary	Tools & Resources
Step 1 Context	• Strategic Objectives Assessment • Threat and Resilience Assessment • Stakeholder and Regulatory Assessment	• Strategic plans • Organisational charts • Interviews • Corporate risk register
Step 2 Leadership	• Establish and communicate roles and responsibilities • Adopt a Business Continuity Policy	• Related frameworks and plans • Organisational charts
Step 3 Planning	• Develop continuity planning approach • Articulate key objectives of the programme	• Professional development training programmes • Risk appetite statement • Corporate risk register • Emergency Management Plans
Step 4 Support	• Develop training and awareness programme • Adopt document management and record keeping protocols • Undertake stakeholder analysis and develop communication templates and plan	• Competencies and training needs analysis • Electronic document and records management system (OURDrive) • Interviews
Step 5 Operation	• Undertake Business Impact Analysis • Assess risks associated with critical functions • Identify minimum resource requirements • Set service availability strategies • Develop Business Continuity Plans • Undertake plan validation exercises	• BIA Survey • Workshops • Interviews • Emergency Management Plans • Walk throughs • Validation Exercises
Steps 6 Performance and Improvement	• Develop and monitor key performance indicators • Act on outcomes of quality and compliance reviews • Undertake post-incident reviews	• Training records and feedback • Audit reports • Debrief reports

Figure 2: Business Continuity Management Framework and Business Continuity Plan development process.

5. Context

The first step in establishing a Business Continuity Management Framework is to undertake a context analysis. It involves the following assessments:

Strategic Objectives Assessment

- Review the vision, mission, and strategic objectives of the University as articulated in the "Strategic Direction to 2020" plan and related Divisional/Faculty strategic plans.
- Review the services and resources associated with the achievement of the University's strategic objectives (all outsourced functions or processes associated with the delivery of services will be included in this assessment).

Information sources include:

- Functional/process audit reports
- Organisational charts
- High level workshops
- Face to face interviews
- Contemporary documents review (i.e. annual reports, key policies)

Threat and Resilience Assessment

- Identify threats and potential impacts on critical services.
- Assess corporate preparedness/ existing continuity initiatives.

Information sources include:

- Scenario analysis
- Corporate Risk Register
- Dedicated risk assessment exercise
- Past incidents and near misses

Stakeholder and Regulatory Assessment

- Identify stakeholders and other interested parties.
- Consider the University's legislative and regulatory obligations.

Information Sources:

- Stakeholder analysis
- Interviews with key staff

6. Leadership

Overall accountability for the development and implementation of the business continuity framework has been assigned to the Vice-Chancellor by the University Council. The Vice-Chancellor has in turn delegated this responsibility to the Chief Operating Officer. Additional business continuity roles and responsibilities are detailed in the Business Continuity Policy which can be found in the Policy Library on the University's website.

7. Planning

The University's approach to business continuity is essentially process-centric or activity-orientated. The framework and underlying activities are designed to minimize the likelihood and impact of threats to core corporate, academic, and research operations. The framework does however recognize that the 'soft' issues of positive staff behaviours and actions can contribute significantly to continuity efforts. On that basis the framework places significant emphasis on staff training and awareness activities, particularly as they relate to legal and regulatory obligations (consider health and safety) and communication protocols (to ensure early warning signals are transmitted to management quickly and efficiently).

Objectives

Business continuity objectives and associated measures are summarised in the following table:

Objective	**Measure**
1. Gain executive commitment	- Member of the senior leadership team appointed as the business continuity champion - Business Continuity Policy endorsed by executive
2. Maintain and enhance skills of staff responsible for business continuity activities	- Number of courses attended per year. - Achievement of business continuity competency objectives detailed in staff performance and development plans.
3. Define the business impacts of critical services	- Business Impact Analysis – identification of critical functions together with recovery time objectives, resources requirements, minimum levels of service.
4. Identify and evaluate threats to key operations	- Risk assessment. - Documented risk mitigation strategies for key operations not covered by continuity plans.
5. Incident management structure established	- Incident communication protocols in place. - Incident management teams in place.
6. Business continuity plans developed	- Recovery procedures for each campus documented. - Procedures validated by exercises.
7. Business continuity team members familiar with roles and responsibilities	- Observation during validation exercises. - Post-exercise debrief and feedback.
8. Corporate business continuity capability maintained	- Business Continuity Policy and plans up-to-date. - Cyclical plan for validation exercises in place.

In order to keep the implementation of the framework manageable, business continuity plans will be developed using a campus-based approach. The risks associated with the loss of critical functions will be subject to a formal risk assessment. The outcomes of the assessment will be used to prioritise functions and the subsequent development of continuity plans. Contingency plans/risk mitigations strategies will also be developed for significant functions not included in the plans. It is anticipated that as the programme matures these significant functions will be progressively included in continuity plans as the plans are updated/revised.

8. Support

Awareness and Training

To increase the knowledge and skills of staff, awareness and training activities will be conducted on a regular basis with the following target audiences:

- Senior Management – in the form of briefings to help them understand their business continuity leadership role.
- Staff with specific business continuity responsibilities – fire evacuation wardens, health and safety staff, Campus Watch, and others detailed in the 'Roles and Responsibilities' contained in the Business Continuity Policy.
- General staff – basic knowledge about the value of business continuity initiatives, information that complements emergency management training.
- Critical vendors – raise awareness of the University's business continuity programme, specific training may be required to raise vendor capabilities.

Training will cover the overlapping duties associated with emergency management planning and business continuity plan activation/stand-down procedures. The training be facilitated by the Office of Risk, Assurance and Compliance. Additional ad-hoc training will also be provided as required/on request.

Documentation

Business continuity related documentation will be protected to ensure there is no loss of confidentiality or integrity. It will be maintained on the University's electronic document and records management system (OURDrive) and be readily available for use by authorised staff.

Version controls will be applied by the system to prevent the unintended use of obsolete information and the distribution of confidential hardcopy documents will be controlled.

Backup copies of key documents (both electronic and hardcopy) will be maintained for each campus at a secondary site.

Internal and External communications

As part of the implementation of the Business Continuity Management Framework, communication protocols will be developed for staff, students, stakeholders (including the community and media), suppliers, and contractors.

<u>Communication Templates</u>

Although the content, timing, and recipients of information disseminated during a disruptive incident will vary according to circumstances, communication templates will be prepared in advance and maintained.

Key messages may include:

- How the University is maintaining “business-as-usual”
- The University’s key priorities, whilst ensuring the ongoing safety and well-being of students and staff affected by the incident.
- Where and when further information updates can be found regarding the University’s management of the incident.
- How the incident affects them (the safety and welfare of people are of the utmost importance)
- How they can support recovery efforts (their roles in the business continuity and recovery process)
- Alternative forms of working (alternate locations or working from home)

Communications Plan

A Communications Plan will also be developed to ensure that:

- All stakeholders and interested parties have been identified.
- Consistent messages are sent to relevant stakeholder groups.
- Messages are sent out at times and with a frequency that supports business continuity recovery objectives.

The template provided in Appendix 4 can be used to develop the communications approach. The communications plan will link to business continuity plans and provide a summary of key communications proposed during the period of disruption. When developing these communications the need to maintain the confidence of key stakeholders and demonstrate the University’s business continuity capability, should be taken into consideration.

Communications will include:

- Regular reports on the status of the recovery of critical functions and services for the Council, Audit & Risk Committee, senior leadership and senior management (where the effects of a disruption are protracted).
- Reports to staff, students, and other stakeholders.
- Invitations to information sessions (where the effects of a disruption is protracted).
- Articles to be included in staff newsletters, social media, print media.

Emergency Services/External Agencies

The University will work jointly with external agencies to identify information requirements such as warnings, incident updates and recovery strategies and incorporate these requirements into its business continuity communication protocols. This work will help to establish a mutual understanding of the roles and actions each organisation takes during an incident.

Implementation and Operation of the Business Continuity Management Framework

9. Operation

9.1 Business Impact Analysis

The Business Impact Analysis (BIA) helps to determine the recovery priorities, objectives, and targets of the business continuity programme. During the analysis, the activities that support the provision of services are identified and the impacts over time of not performing these activities is considered. Elements of the BIA include:

a) Identification and Classification of Key Functions

The purpose of the evaluation is to assess what critical functions need to be recovered and in what order of priority. Decisions should be made in accordance with legal/regulatory and health and safety requirements and include a consideration of available resourcing and the University's appetite for risk.

Critical functions are directly responsible for the delivery of services; these functions enable the University to achieve its strategic objectives and comply with legal and regulatory requirements.

Critical-supporting functions provide outputs to critical functions, without which the critical function could not operate. If they are the only source of supply to the critical function they are classified as single points of failure.

Supporting functions provide support to the critical and critical-supporting functions. Their failure during an incident does not immediately compromise the University's ability to achieve its strategic objectives and comply with legal and regulatory requirements.

When deciding what constitutes a critical function, consideration is given to the University's key objectives and obligations and how they are achieved. The outputs required to meet these objectives and obligations are identified during the BIA together with the underlying functions that deliver those outputs. This process also includes an evaluation of the timeframes in which the objectives and obligations need to be achieved.

b) Assessment of Recovery Timeframes

Prioritised timeframes for the resumption of critical functions are established and incorporated into subsequent planning activities i.e.

- **Maximum Tolerable Period of Disruption (MTPD)**, the maximum time period that the University could operate without a critical function, after which the impact would become unacceptable.
- **Recovery Time Objective (RTO)**, the time period in which a critical function must be recovered. Note - The RTO should always be shorter than the MTPD.
- **Recovery Point Objective (RPO)**, the point in time in which key activities should be restored to after an incident, i.e. consider data integrity and information technology system outages.

c) Identification of Dependencies

The identification of dependencies and the supporting resources for these activities assist in the prioritisation of critical functions and recovery strategies. Dependencies include suppliers, contractors and outsourcing partners.

d) Information Collection

The most common data collection methods are questionnaires, personal interviews and documentary reviews. These activities are undertaken prior to the workshops where the BIA outcomes are evaluated and endorsed.

The outputs of the BIA include:

- A prioritised timeline of activities for the recovery of the University's critical functions.
- A Business Continuity Resource Requirements Analysis (BCRRA) containing the necessary resources to achieve the prioritised recovery of critical functions (refer Part 9.4 below, Evaluation and Selection of Business Continuity Strategies).
- A list of internal and external dependencies of critical functions.

The BIA will be refreshed/undertaken on at least an 18 monthly basis to ensure continuity strategies remain relevant and focused.

9.2. Risk Assessment

After identifying critical functions and supporting resources the next stage in the process is a risk assessment. A risk assessment is undertaken to ensure that business continuity efforts are focussed on those critical functions most at risk and that would have the greatest impact on the University. It is also used to develop an understanding of the interdependencies amongst different critical functions in order to determine single points of failure or areas where there is a high concentration of risk.

Business continuity risk assessments use established risk assessment techniques as described in the University's Risk Management Framework. A copy of the framework can be found on the University's website.

An alternative and less resource intensive approach is to undertake a detailed review the University's risk registers. This activity also provides an overall view of the risk profile of the University and its divisions.

9.3 Resource Requirements Analysis

This activity identifies the minimum resources required to maintain critical functions and together with the BIA, assists in the further development of business continuity strategies.

The following considerations should be taken into account when undertaking the analysis.

a) People

- Training – transfer/develop core skills associated with the delivery of critical functions amongst a wider group of staff.
- Diversification – different work locations for key staff, separate travel arrangement plans.
- Procedures and guidelines – document how critical functions are performed.
- Succession planning – identify backup staff.
- Specialist third parties – engagement of contractors to perform critical functions.

b) Premises

- Secondary locations – alternate work locations to house critical functions.
- Flexible working arrangements – temporary arrangements using business centres, client offices and working from home.
- Reciprocal arrangements – agreements with other organisations to share each other's premises and facilities.

c) Information

- Backup and recovery – methods and effectiveness of recovery processes.
- Confidentiality of information – adequacy of safeguards.
- Availability – information format, hardcopy or electronic, and storage locations.
- Currency – accuracy and reliability of information.

d) Technology

- Power – the provision of an uninterrupted power system (UPS) for critical technology or infrastructure.
- Network – voice and data communications and network availability.
- Backup storage – security and portability.
- Hardware and software – backup, repair, replace, or temporary loan options.

Note – the University has a Disaster Recovery Plan that addresses strategic/major technology risks. Information Technology Services should be consulted if the identified technology requirements are significant or if any uncertainties exist in terms of resourcing.

e) Supplies

- Buffer stocks – emergency supplies.
- Contractual agreements – arrangements with third-party suppliers to deliver stocks on short notice.
- Alternative sourcing – availability of a wide selection of critical suppliers.
- Validation of business continuity – suppliers to demonstrate business continuity capability (ensures resilience in supply chain network).

9.4 Evaluation and Selection of Business Continuity Strategies

A business continuity strategy describes how the University will recover each critical function within the Recovery Time Objective established during the Business Impact Analysis activity. It details resourcing requirements and sets out how relationships with key stakeholders will be managed at the time of disruption.

Availability of Services

There are three levels at which strategies can be set:

- **Full availability** – critical services cannot fail.
- **Critical services recovered within RTO's** (Recovery Time Objectives) at an agreed minimum level.
- **Suspend** critical functions.

If the strategy chosen is to suspend a critical function during a disruption a communication protocol should be developed for informing stakeholders who have an interest in the critical function that is to be suspended.

Strategy Selection

The following factors should be considered when evaluating and selecting a strategy for each critical function:

- Business requirements.
- The agreed recovery time objectives (RTO's).
- The maximum tolerable period of disruption for each service.
- The key resources required, e.g. people, premises, technology, information, and supplies.
- Costs of implementing the strategies compared to the speed of recovery.
- Recovery phase (partial or full resumption).
- Consequences of inaction.
- The business impact analysis and risk assessments.

Consolidation of Recovery Resources

This activity re-evaluates the resources needed to implement continuity strategies associated with each critical function. It ensures that the resources associated with continuity strategies do not conflict with one another are reasonable and achievable and/or fall within predetermined continuity budgets. The outcomes of the consolidation process are summarised in Business Continuity Resource Requirements Analysis (BCRRA).

Approval

Business continuity strategies are to be agreed with and signed off by the head of each Division and then submitted to the Vice-Chancellor for endorsement before Business Continuity Plans are developed.

9.5 Business Continuity Plans

Business Continuity Plans contain the procedures necessary for the maintenance of critical functions. They provide the staff with the information needed for an immediate response to a disruptive incident and to access the resources needed to implement predetermined continuity strategies.

The University operates across multiple locations and on that basis has adopted campus-based plans in which the critical functions of the campus as a whole are considered when formulating and prioritising responses to disruptive incidents. The plans are not intended to address every eventuality as the nature of individual incidents may vary. Responses to disruptions therefore need to be flexible in approach and actions may need to be adapted according to the circumstances.

Business Continuity Plans outline:

- Purpose and scope.
- Objectives.
- Activation criteria and procedures.
- Outline specific steps to be taken during a disruption.
- Roles, responsibilities, and authorities.
- Internal and external communication requirements and procedures – media, staff, students, and stakeholders.
- Internal and external interdependencies and interactions.

- Resource requirements.
- Information flow and documentation processes.
- Stated assumptions and identification of dependencies.
- A process for standing down once the incident is over.

Business Continuity Plan Activation

Business continuity plan activation and stand-down (following resumption of normal activity) will be consistent with the authorities detailed in the Emergency Management Policy, Emergency Management Plan and Business Continuity Policy. The authority to activate business continuity plans rests with the Vice- Chancellor/Incident Controller/Chief Operating Officer. For campuses in Christchurch and Wellington the Incident Controller is the Business and Operations Manager, unless otherwise directed by the Dean of the campus. The Incident Controller in Invercargill is the Operations Coordinator.

It is anticipated that in the majority of instances the activation of business continuity plans will be one of many coordinated actions taken by the Vice-Chancellor/Incident Controller/Chief Operating Officer in response to an emergency or disruption to services on campus. On that basis staff are expected to escalate any matters involving a campus emergency or disruption to services to management and/or the Proctor's Office - the procedures detailed in the Business Continuity Framework and Business Continuity Plans support (do not replace) these established communication pathways.

9.6 Relationship to Emergency Procedures

The University's emergency procedures and the activities detailed in Business Continuity Plans do not operate independently of each other. This is to ensure delays, conflicts, incorrect allocation of resources and failure to achieve required levels of continuity are avoided.

The emergency procedures are defined in the Emergency Management Plan and Emergency Procedures flip chart.

During a disruption a Business Continuity Management Team will operate independently from both the Incident Management Team and/or the Strategic Emergency Management Group. The Business Continuity Management team will however maintain close communications with the Incident Management Team and/or the Strategic Emergency Management Group to ensure recovery efforts are coordinated.

Please note that emergencies and incidents should still be reported in accordance with the procedures detailed in the Emergency Procedures flip chart.

9.7 Business Continuity Plan Validation

The purpose of plan validation is to develop staff skills and confidence and to assess the quality of the Business Continuity Plan and associated activities. Exercises are designed to identify false assumptions and unrealistic recovery time objectives. The exercises can also be used to involve and assess the overall business continuity capability of critical suppliers.

An important component of an exercise is the testing of communications intended to be used during a disruption i.e. availability and alternatives.

The exercises will also be based on realistic scenarios with clearly defined aims and objectives.

When commencing an exercise appropriate staff and stakeholders will be notified prior to the exercise (i.e. Campus Safety, reception areas). This will help to avoid situations where the exercise could be mistaken for a real event and create a disruption. On that basis procedures for aborting an exercise will also be considered prior to the exercise commencing.

Following an exercise, debriefs will also be held to identify lessons learned and opportunities for improvement.

Exercises will be matched to the business continuity maturity level of the University.

Monitoring and Improving the Business Continuity Management Framework

10. Performance Evaluation and Improvement

The following Key Performance Indicators (KPI's) will be maintained and reported to the Audit & Risk Committee:

KPI	**Measure**	**Frequency**
Tests and debriefs conducted	Count	Quarterly
Workshops and training sessions	Count	Quarterly
% of plans updated within the last 12 months	% and Count	Quarterly

The programme will also be independently audited to ensure it confirms to the requirements articulated in the Business Continuity Policy and the broader directions maintained in the Business Continuity Management System Standard ISO 22301:2012.

If Business Continuity Plans have been activated in response to a disruption a post-incident review will be conducted and the outcomes used to improve/strengthen associated procedures and activities.

11. Contact Information

For further information regarding the Business Continuity Management Framework contact the Office of Risk, Assurance and Compliance at risk.management@otago.ac.nz

Glossary of Terms

Activity

Process or set of processes undertaken by an organisation (or on its behalf) that produces or supports one or more products and services.

Business Continuity

Capability of the organisation to continue delivery of products or services at acceptable predefined levels following disruptive incident.

Business Continuity Management

Holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

Business Continuity Plan

Documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.

NOTE Typically this covers resources, services and activities required to ensure the continuity of critical business functions.

Business Impact Analysis

Process of analysing activities and the effect that a business disruption might have upon them.

Event

An incident, occurrence or change of a particular set of circumstances, a situation that might be, or could lead to, a disruption, loss, emergency or crisis.

Exercise

Process to train for, assess, practice, and improve performance in an organisation.

Stakeholder

Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

Maximum Tolerable Period of Disruption (MTPD)

Time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable.

Prioritised Activities

Activities to which priority must be given following an incident in order to mitigate impacts.

Recovery Point Objective (RPO)

Point to which information used by an activity must be restored to enable the activity to operate on resumption, usually applied to data held on information technology systems.

NOTE Can also be referred to as “maximum data loss”.

Recovery Time Objective (RTO)

Period of time following an incident within which:

- product or service must be resumed, or
- activity must be resumed, or
- Resources must be recovered.

NOTE For products, services and activities, the recovery time objective must be less than the MTPD

Resources

All assets, people, skills, information, technology (including plant and equipment), premises, 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.

Risk Appetite

Amount and type of risk that an organization is willing to pursue or retain.

Source: *Societal security – Business Continuity Management Systems – Requirements, ISO 22301:2012*

Appendices:

1. Disruptive Events
2. Business Impact Analysis Template
3. Risk Rating/Classification Table
4. Communication Plan Template
5. Business Continuity Plan Validation Programme

Disruptive Events Appendix 1

Examples of events that could seriously impact critical corporate, academic and research functions:

People	• Shortage of staff • Prolonged industrial dispute • Bomb threat/ serious act of violence
Premises	• Loss of facility • Denial of access to premises • Utility failure (i.e. electricity, water)
Technology	• Prolonged loss of network • Loss of data • Cyber attack
Supplies	• Failure of key supplier • Failure of outsourced provider • Loss of critical resources
Environmental	• Flood, earthquake, or fire • Pandemic • Serious contamination/Hazmat incident

Business Impact Analysis

Appendix 2

Campus:	**Division:**	**Department/Office:**	**Completed by:**	**Date:**

Critical Function	Critical Time Periods	Resources	Dependencies	RTO	MTPD
Consider strategic objectives, regulatory requirements, health and safety	*- Admissions/ enrolments* *- Examinations/ results processing*	*People - Key staff, minimum staffing level* *Premises - Essential facilities, equip, workstations* *Information - Documents, files, records, manuals* *Technology - Computers, printers, applications, data*	*Internal: Other departments/ individuals* *External: Outsource, contractors, supplier*	*Recovery Time Objective*	*Maximum Tolerable Period of Disruption*

Appendix 3

Overall Risk (L X I)	Likelihood (L)	Impact (I)	Risk Rating/Classification - Corporate/Division	Required Action
Very High **≥ 15**	(5) Almost Certain • *Will undoubtedly happen* • *Greater than 80% chance*	(5) Very Serious	• Potential financial impact of $10,000,000 (Corp.)/$1,000,000 (Div.) or more in any 12 mth period • Detrimental impact on operations or major projects • Sustained loss in reputation • Sustained impact on services delivery or quality • Loss of public confidence in the University • Contractual, legislative, or regulatory non-compliance with certain litigation • Life threatening	• Immediate notification to Audit & Risk Committee • Requires immediate VC/DVC/PVC/Senior Management attention • Requires a detailed risk treatment plan within 30 days
High **10 – 14**	(4) Probable • *Will probably happen* • *50 - 80% chance*	(4) Serious	• Potential financial impact of $5,000,000 (Corp.)/$500,000 (Div.) or more in any 12 month period • Major impact on operations or major projects • Serious loss in reputation • Serious impact on services or quality • Probable loss of public confidence in the University • Contractual, legislative, or regulatory non-compliance with probable litigation • Extensive injuries	• Requires prompt senior management action/ attention • Requires a detailed risk treatment plan within 60 days • Reported to Audit & Risk Committee
Medium **5 – 9**	(3) Likely • *Might happen* • *20 - 50% chance*	(3) Moderate	• Potential financial impact of $2,000,000 (Corp.)/$200,000 (Div.) or more in any 12 month period • Moderate impact on operations or major projects • Short-term loss in reputation • Moderate decline in services or quality • Possible loss of public confidence in the University • Contractual, legislative, or regulatory non-compliance with potential for litigation • Minor injuries	• Requires ongoing management of control effectiveness • Manage by specific monitoring or response procedures • May require a risk treatment plan
Low **3 - 4**	(2) Unlikely • *Not expected to happen* • *5 - 20% chance*	(2) Minor	• Potential financial impact of $1,000,000 (Corp.)/$100,000 (Div.) or more in any 12 month period • Minor impact on operations or major projects • No loss in reputation • Minor impact on services or quality • No loss of public confidence in the University • Contractual, legislative, or regulatory non-compliance but litigation unlikely • Potential for injury	• Manage by routine procedures • Monitor control effectiveness by local management • May require a risk treatment plan
1 - 2	(1) Rare • *Less than 5% chance.*	(1) Negligible	• Potential financial impact of $1,000,000 (Corp.)/$100,000 (Div.) or less in any 12 month period	• Impact to be absorbed by daily business running costs or managed through routine procedures

Overall Risk	Likelihood (L)	Impact (I)	Health and Safety
Very High **> 15**	(5) Almost Certain	(5) Very Serious	Life threatening: • Loss of life(s) • Major health and safety incident involving staff or members of the public • Permanent disability • Permanent ill-health
High **10 - 14**	(4) Probable	(4) Serious	Extensive injuries: • Loss of life • Significant health and safety incident involving staff or members of the public • Multiple serious injuries • Long term illness/disability
Medium **5 - 9**	(3) Likely	(3) Moderate	Minor injuries: • Possible hospitalisation • Numerous days lost • Short term illness
Low **3 - 4**	(2) Unlikely	(2) Minor	Potential for injury: • Medical/ First Aid treatment required • Some days lost
Near Miss **1 - 2**	(1) Rare	(1) Negligible	No injuries: • Report, record and review.

Overall Risk	Likelihood (L)	Impact (I)	Project Management
Very High **≥ 15**	(5) Almost Certain	(5) Very Serious	Detrimental impact on operations or major projects: • Capital cost impact – *specific to project* • Recurrent cost impact exceeds $5,000,000 • 3 months slippage • Catastrophic impact on project objectives, identified benefits, deliverables • Multiple irreversible injuries/illness or
High **10 - 14**	(4) Probable	(4) Serious	Major impact on operations or major projects: • 1 Capital cost impact – *specific to project* • Recurrent cost impact exceeds $1,500,000 • 2 months slippage • Significant impact on project objectives, identified benefits, deliverables • Irreversible injury/illness, permanent disability or fatality
Medium **5 - 9**	(3) Likely	(3) Moderate	Moderate impact on operations or major projects: • Capital cost impact – *specific to project* • Recurrent cost impact exceeds $300,000 • 1 month slippage • Some impact on project objectives, identified benefits, deliverables • Serious injury/illness – lost time of more than 4 days
Low **3 - 4**	(2) Unlikely	(2) Minor	Minor impact on operations or major projects: • 1Capital cost impact – *specific to project* • Recurrent cost impact exceeds $75,000 • 2 weeks slippage, • Small impact on project objectives, identified benefits, deliverables • Injury/ illness – lost time of less than 4 days
1 - 2	(1) Rare	(1) Negligible	• Capital cost impact – *specific to project* • Recurrent cost impact less than $75,000

Communications Plan Template Appendix 4

Stakeholders/ Target Audience	**Purpose/ Objective of Communication**	**Key Message/ Content**	**Communication Channel/ Method**	**Timing/ Date**	**Frequency**	**Communication Prepared By**	**Communication Approved By**	**Status**
Internal:								
Council								
Vice-Chancellor								
Management								
All Staff								
Specific Depts/Divisions								
Students								
External:								
Government agencies								
Business Partners /Suppliers								
Other Institutions								
Media								

Business Continuity Plan Validation Programme Appendix 5

The following are a series of activities that tests different components of the business continuity plans. The program encompasses all of the University's campuses.

Element	Description	Frequency	Duration	Prerequisite	Responsibility
Call Tree & Notification Exercise	An exercise to be run during and outside business hours to test the notification and call tree procedures contained in the Business Continuity Plans. This will aid verification of call tree procedures and reliability of contact details/ availability of key staff.	1 x per year	1-2 hours	None	Office of Risk, Assurance and Compliance
BCP Training / Familiarisation	Key employees will undergo general business continuity training, detailing the content and objectives of the plans. Key employees with an active role in plan activation procedures will be involved in a more detailed a BCP walkthrough / training exercise session.	1 x per year	2-3 hours	None	Office of Risk, Assurance and Compliance
Desktop Exercise	Desktop exercises will be a progressive event involving the application of varying scenarios to test different business functions. This will be an opportunity for employees with an active role to retain and upgrade their skills and knowledge of business continuity and continuity strategies.	1 x per year	2-3 hours	BCP Training/ Familiarisation	Office of Risk, Assurance and Compliance
Simulation Exercise	The simulation exercise will be a comprehensive scenario based exercise conducted at each campus and focused on major risks faced by each campus. It will involve third parties where appropriate i.e. Police, Fire, Ambulance. These exercises will be undertaken when the framework is sufficiently mature.	1 every 2 years	4 hours	BCP Training/ Familiarisation	Office of Risk, Assurance and Compliance