BUSINESS CONTINUITY MANAGEMENT FRAMEWORK

<table>
<thead>
<tr>
<th>Approving authority</th>
<th>University Council</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval date</td>
<td>5 August 2013 (3/2013 meeting)</td>
</tr>
<tr>
<td>Advisor</td>
<td>Colin McAndrew</td>
</tr>
<tr>
<td>Next scheduled review</td>
<td>2018</td>
</tr>
<tr>
<td>TRIM document</td>
<td>2013/0014764</td>
</tr>
</tbody>
</table>
Table of Contents

1. Lexicon of Terms ........................................................................................................................................... 3
2. Glossary of Acronyms ................................................................................................................................. 6
3. INTRODUCTION ............................................................................................................................................... 7
   3.1. What is Business Continuity? .................................................................................................................. 7
   3.2. What is BCM? .......................................................................................................................................... 7
   3.3. Why is BCM important? ......................................................................................................................... 8
   3.4. What is the business continuity planning concept? .................................................................................. 8
   3.5. What is disruption-related Risk? .............................................................................................................. 9
   3.6. What is a resilience capability and why is it important? ....................................................................... 10
4. SCOPE AND APPLICATION OF THE FRAMEWORK .................................................................................. 11
   4.1. Introduction ............................................................................................................................................ 11
   4.2. BCM Policy ........................................................................................................................................... 11
   4.3. Objective of the Framework ................................................................................................................... 11
   4.4. Roles and Responsibilities ..................................................................................................................... 12
   4.5. Communication of BCM. .................................................................................................................... 12
5. BCM PROGRAMME ......................................................................................................................................... 13
   5.1. Introduction ............................................................................................................................................ 13
   5.2. Business Continuity Planning Methodology .......................................................................................... 14
      5.2.1. Step 2: Risk and Vulnerability Analysis .......................................................................................... 15
      5.2.2. Step 3: Business Consequence Analysis ....................................................................................... 16
      5.2.3. Step 4: Define Response Strategies .............................................................................................. 16
      5.2.4. Step 5: Developing Resource and Interdependency Requirements .............................................. 17
      5.2.5. Step 6: Develop Business Continuity Plans ................................................................................. 17
      5.2.6. Step 7: Develop a Communication Strategy ................................................................................ 18
      5.2.7. Step 8: Training, Testing and Maintaining Plans ......................................................................... 18
      5.2.8. Step 9: Activation and Deployment of Plans ............................................................................... 20
6. LINK BETWEEN BCP, EMERGENCY, CRISIS AND DISASTER RECOVERY PLANNING .......... 21
   6.1. Introduction ............................................................................................................................................ 21
7. FRAMEWORK MAINTENANCE AND ASSURANCE ..................................................................................... 23
8. REPORTING .................................................................................................................................................. 23
9. RESOURCES .................................................................................................................................................. 23
1. **Lexicon of Terms**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptation</td>
<td>Refers to the University capability to cope with uncertainty, change and associated stresses, and adjust to change</td>
</tr>
<tr>
<td>Business Continuity (BC)</td>
<td>A state of continued, uninterrupted operation of a business in all contexts.</td>
</tr>
<tr>
<td>Business Continuity Management (BCM)</td>
<td>“A holistic process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause. It provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of key stakeholders, reputation, brand and value-creating activities.” (ISO 22301). BCM is an integral part of the University’s risk management effort to manage disruption-related risk and respond to emergencies.</td>
</tr>
<tr>
<td>Business Continuity Management Programme</td>
<td>“Ongoing management and governance process supported by top management and appropriately resourced to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products and services through training, exercising, maintenance and review.” (Business Continuity Institute)</td>
</tr>
<tr>
<td>Business Continuity Management Lifecycle</td>
<td>“A series of business continuity activities which collectively cover all aspects and phases of the BCM programme.” (Business Continuity Institute)</td>
</tr>
<tr>
<td>Business Continuity Plan (BCP)</td>
<td>An output of BCM. This process leads to a clearly defined and documented plan which sets out the procedures, resources and systems necessary to continue or restore the activities of an organisation should unpredicted business disruption occur. The BCP is used as a communication and decision support tool and is executed in response to a business disruption.</td>
</tr>
<tr>
<td>Business Impact Analysis</td>
<td>“The process of analysing business functions and the effect that a business disruption might have upon them.” (Business Continuity Institute). The BIA provides a level of analysis to examine in detail any consequences that may exceed routine management capability.</td>
</tr>
<tr>
<td>Communication and Consultation</td>
<td>“Continual and iterative processes that an organisation conducts to provide, share or obtain information, and engage in dialogue with stakeholders regarding the management of disruption-related risk.” (AS/NZS 5050: 2010)</td>
</tr>
<tr>
<td>Context</td>
<td>“The external and internal parameters to be taken into account when managing disruption-related risk and setting the scope and risk criteria for the BCM Policy.” (AS/NZS 5050: 2010)</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Control</td>
<td>An existing process, policy, device, practice or other action that acts to minimise negative risks or enhance positive opportunities. May also be applied to a process designed to provide reasonable assurance regarding the achievement of objectives. (AS/NSS ISO 31000:2009)</td>
</tr>
<tr>
<td></td>
<td>Business Continuity controls ensure an uninterrupted availability of key business resources that support the continuation of key or crucial business processes and objectives.</td>
</tr>
<tr>
<td>Consequence</td>
<td>Outcome of an event, determined in relation to the achievement of objectives. The outcome can be positive or negative and expressed quantitatively or qualitatively. In addition, there can be more than one consequence from one event. (AS/NSS ISO 31000:2009)</td>
</tr>
<tr>
<td>Corporate Governance</td>
<td>Primarily concerned with, but not limited to:</td>
</tr>
<tr>
<td></td>
<td>• Effectiveness and efficiency of operations;</td>
</tr>
<tr>
<td></td>
<td>• Compliance with laws and regulations;</td>
</tr>
<tr>
<td></td>
<td>• Vulnerability of the organisation and safeguarding of assets.</td>
</tr>
<tr>
<td></td>
<td>Governance has specific implications for BCM, as the availability and integrity of information and continuity of services are key internal control concepts directly attributable to effective BCM.</td>
</tr>
<tr>
<td>University Council</td>
<td>The Council of Griffith University.</td>
</tr>
<tr>
<td>Crisis</td>
<td>Any event that is, or might lead to, an unstable or dangerous situation affecting an individual or group.</td>
</tr>
<tr>
<td>Disruption-related risk</td>
<td>University consequences of being unable to remain operational. Refers to how quickly or severely an outage could affect achievement of University time sensitive objectives.</td>
</tr>
<tr>
<td></td>
<td>Disruption related risk management is a particular application of risk management.</td>
</tr>
<tr>
<td>Event</td>
<td>An incident or situation, which occurs in a particular place during a particular interval of time.</td>
</tr>
<tr>
<td>Hazard</td>
<td>A source of potential harm or a situation with a potential to cause loss. The words ‘threats’ and ‘hazards’ are often interchangeable.</td>
</tr>
<tr>
<td>Likelihood</td>
<td>Used as a qualitative description of probability or frequency of a risk occurring.</td>
</tr>
<tr>
<td>Loss</td>
<td>Any negative consequence, financial or otherwise. Can be differentiated as follows;</td>
</tr>
<tr>
<td></td>
<td>• <strong>Maximum foreseeable loss</strong> - highest possible loss after considering controls</td>
</tr>
<tr>
<td></td>
<td>• <strong>Maximum possible loss</strong> – highest possible loss without considering controls</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Maximum Acceptable Outage</strong></td>
<td>The duration after which the University’s viability will be threatened if a service or function cannot be resumed.</td>
</tr>
<tr>
<td><strong>Mitigation</strong></td>
<td>Involves pre-empting a challenge and taking steps to avoid the threat or limit any negative consequence.</td>
</tr>
<tr>
<td><strong>Probability</strong></td>
<td>The likelihood of a specific event or outcome, measured by the ratio of specific events or outcomes to the total number of possible events or outcomes.</td>
</tr>
<tr>
<td><strong>Recovery</strong></td>
<td>“Steps taken to resume the business within an acceptable timeframe following a disruption.” (Business Continuity Institute)</td>
</tr>
<tr>
<td><strong>Recovery Point Objective</strong></td>
<td>“The target set for the status and availability of data (electronic and paper) at the start of a recovery process. It is a point in time at which data capacity of a process is in a known, valid state and can safely be restored from.&quot; In purely IT DR terms it can be seen as the precise time to which data and transactions have to be restored. (Business Continuity Institute)</td>
</tr>
<tr>
<td><strong>Recovery Time Objective</strong></td>
<td>“The target time for resuming the delivery of a product or service to an acceptable level following its disruption.” (Business Continuity Institute)</td>
</tr>
<tr>
<td><strong>Residual risk</strong></td>
<td>The remaining risk after management has taken action to alter the risk’s likelihood or impact.</td>
</tr>
<tr>
<td><strong>Resilience</strong></td>
<td>The University's ability to achieve its immediate objectives in uncertain and non-routine times.</td>
</tr>
<tr>
<td><strong>Risk</strong></td>
<td>The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.</td>
</tr>
<tr>
<td><strong>Risk analysis</strong></td>
<td>A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.</td>
</tr>
<tr>
<td><strong>Risk appetite</strong></td>
<td>The level of risk that is acceptable to the board or management. This may be set for the University as a whole, for different groups of risks or at an individual risk level. Considerations include:</td>
</tr>
<tr>
<td></td>
<td> - Spatial distribution</td>
</tr>
<tr>
<td></td>
<td> - Temporal distribution</td>
</tr>
<tr>
<td></td>
<td> - Intensity (how big/fast/powerful)</td>
</tr>
<tr>
<td></td>
<td> - Manageability</td>
</tr>
<tr>
<td><strong>Risk assessment</strong></td>
<td>The overall process of risk analysis and risk evaluation.</td>
</tr>
<tr>
<td><strong>Risk Criteria</strong></td>
<td>“Terms of reference against which the significance of a risk is evaluated. Risk criteria are based on internal and external context, are regularly reviewed to ensure continued relevance. Risk criteria can be derived from standards, laws and policies.” (Business Continuity Institute)</td>
</tr>
<tr>
<td><strong>Risk Management Framework</strong></td>
<td>The totality of the structures, methodology, procedures and definitions that the University has chosen to use to implement its Risk Management Processes.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Risk Register</td>
<td>The means by which the University elects to manage or treat the individual risks. The main categories are to accept the risk; to mitigate it by reducing its impact or likelihood; to transfer it to another organisation or to avoid the activity creating it.</td>
</tr>
<tr>
<td>Stakeholders</td>
<td>Those people and organisations who may affect, be affected by, or perceive themselves to be affected by, a decision or activity.</td>
</tr>
<tr>
<td>Vital Records</td>
<td>“Any information documents or data deemed essential for recovery from a disaster or major incident.” (Business Continuity Institute)</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>The degree to which a person, asset, process, information, infrastructure or other resources are exposed and susceptible to the actions or effects of a hazard, event or risk.</td>
</tr>
</tbody>
</table>

2. **Glossary of Acronyms**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BC</td>
<td>Business Continuity</td>
</tr>
<tr>
<td>BCM</td>
<td>Business Continuity Management</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Plan</td>
</tr>
<tr>
<td>HB</td>
<td>Handbook (Australian Standards)</td>
</tr>
<tr>
<td>IT DR</td>
<td>Information Technology Disaster Recovery</td>
</tr>
<tr>
<td>MAO</td>
<td>Maximum Acceptable Outage</td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time Objective</td>
</tr>
</tbody>
</table>
3. **INTRODUCTION**

3.1 **What is Business Continuity?**

Business continuity (BC) refers to a state of continued, uninterrupted operation of a business in all contexts. It focuses on the resiliency of people, property, processes, platforms and providers as well as the availability and integrity of information.

A business continuity plan is invoked after a disruptive event occurs – it is not about preventing a disruptive event from occurring. This disruptive event is normally a very low probability but very high consequence event. The cause of the disruption is irrelevant in business continuity management.

3.2 **What is BCM?**

Management of disruption-related risk is founded on a thorough understanding of internal, external and risk management contexts the University operates within. As risk management leads to a better understanding of the University and those risks it needs to balance, so BCM reviews how the University functions, its dependencies, vulnerabilities and what is critical to its long-term survival.

Should a change in context occur, with the potential for disruption, the management process determines what information, resources, efforts and timelines are required to maintain critical processes and meet time-sensitive objectives while the situation is stabilised or a new advantage seized.

In essence, BCM is a holistic, integrated management process which provides a framework for building operational resilience with the capability for effective response to business disruption. The practice of BCM promotes asset optimisation and business process streamlining. The key functional elements of BCM are outlined in Figure 1.

*Figure 1: Key Functional Elements of BCM.*

---

BCM is an application of risk management, an integral component of sound corporate governance and an important aspect of emergency preparedness and operational resilience. Effective BCM will safeguard the University's core functions and associated expectations of key stakeholders, assist the University meet legal, regulatory and contractual obligations and protect its reputation.

Individual objectives of BCM are to:

- Keep people safe;
- Reduce the University vulnerability to future business discontinuity;
- Protect vital assets owned by the University and those assets belonging to others for which it carries responsibilities;
- Protect intellectual assets and contracts that place the University in a value chain through suppliers and distributors;
- Preserve the ability to meet stakeholder expectations in a wide range of circumstances, including meeting 3rd party arrangements;
- Reduce reliance on key personnel;
- Provide for an orderly and expedited recovery after a disruptive event; and
- Maintain or gain competitive advantage due to a swift and effective response.

3.3 Why is BCM important?
University business strategies and decisions are based on an assumption business continues as:

- Assets and key process inputs will be delivered or be available as planned;
- Everyone knows what to do;
- What to look for and what to expect in their working environment.

However, every step taken to achieve an objective involves uncertainty, and there's always the chance things will not go according to plan. When disruption occurs, there is usually little time to assess which affected business processes and resources are most vital at that time. Crucial decisions are required quickly to divert resources and ensure sustainability of core teaching, research and development functions whilst recovery is coordinated or a new way of operating is established.

BCM will assist the University prioritise processes and supporting resources, and clarify decision-making. This is necessary to limit any damage to the education of University students, research and development activities, and to protect the University reputation and retain staff and students in the long-term.

3.4 What is the business continuity planning concept?
BC planning is a function within a BC programme. It is a continuous process of identifying hazards and University vulnerabilities, the likelihood of disruption, potential consequence on time-sensitive objectives and strategic success, existing control effectiveness and strategies to improve performance and efficiency. It considers risk over time when usual work areas, staff, assets or processes are not available.

Key concepts of the BC planning process are:

- Understand the business;
- Assess the risks;
- Prepare a business continuity plan (BCP); and
- Test the plan.
**Understand the business**

In order to develop a BCP, a thorough understanding of the business is required. This involves defining the business mission and time-sensitive objectives, identifying critical process inputs and outputs and functional dependencies, prioritising process and resource requirements and determining external supply and contractual arrangements.

**Assess the risks**

Risk assessment is the primary activity in the production of a BCP. The identification, analysis and evaluation of risk is the important early step to understand the probability and potential consequence and associated problems from business disruption, determine risk appetite and scope the need for a BCP.

**Prepare a BCP**

The primary output of the BC Process is a BCP, which is a pre-defined, pre-tested, management approved communication and decision support tool. The plan is executed in response to a business disruption.

**Test the Plan**

In the event of a business disruption, relevant staff must understand what is expected of them. Staff with BCP responsibilities should regularly rehearse their roles to test the BCP practicality, validate its currency, confirm their competence and confidence and test their assumptions around access to resources.

The BC planning process is geared towards providing University Council, as well as University stakeholders, comfort that if the worst happens the University has the capacity to recover quickly, safely and as cost effectively as possible.

**3.5 What is disruption-related Risk?**

Disruption refers to an outage which has a time and business consequence dimension, not day-to-day operational glitches which are managed through standard operating procedures.

Disruption results from an event which interrupts business-as-usual critical processes or operations whether anticipated or not. When it comes to business disruption, it is not a matter of if, but when, how, and how severe.

A business disruption can originate from a host of hazard sources and contexts such as:

| University planned event (e.g. open days) | Medical event, e.g. pandemic |
| Bomb threat | Act of violence |
| Cyber attack/malware | Power failure |
| Utility failure | Security breach |
| Technological innovations and upheavals | Data loss |
| Vandalism | On-site emergency |
| International incident | Industrial action/political changes |
| Failure of critical suppliers/outourcing | Environmental contamination |
| Network system failure | Natural events and forces |
| Fire |  |
Such events will potentially consequence one or more of:

- **People** – lead to loss or unavailability of staff (mass absenteeism) or critical skills;
- **Property** – lead to loss or unavailability of facilities, work space and critical assets;
- **Processes** – disrupt critical processes and distract staff from usual work flow;
- **Platforms** – lead to loss or unavailability of ICT infrastructure;
- **Providers** - disrupt utilities, supply chains, contractual arrangements, dependencies

Non-availability of these assets and processes over time could result in an operational outage. How quickly or severely an outage could affect achievement of University time-sensitive objectives is referred to as disruption-related risk. These risks relate to expenditure and losses including:

- **Safety** – danger to staff, students, contractors, visitors;
- **Revenue** – direct loss, compensatory payments, investment loss;
- **Finance** – loss of cash flow, payment guarantees, credit rating;
- **Legal and regulatory** – contractual penalties, liabilities, increased re-insurance costs, failure to meet reporting obligations, increase in regulatory scrutiny;
- **Extraordinary expenses** – need for temporary employees, additional equipment, rental, logistics, travel expenses in order to stabilise situation;
- **Dependencies** – unable to meet customer expectations, supply chain, contracts;
- **Reputation** – unable to meet public image, brand name, sector image, consequence on ratings, ministerial enquiry.

Realisation of these risks individually or in combination could delay achievement of time-sensitive business objectives and, as a cumulative effect, potentially threaten the University's strategic success. The University needs to have a considered and tested method of treating disruption-related risk in the most effective way to meet the University's defined priorities.

### 3.6 What is a resilience capability and why is it important?

Griffith University is a complex, interrelated system of dynamic processes operating in an increasingly uncertain, unpredictable global environment. Resilience capability refers to the system ability to cope with uncertainty, change and associated stresses (implying it is adaptive). A resilient system is able to effectively adjust its functioning in anticipation of, during, or following changes and disturbances, so that it can continue to perform as required after a disruption or a major mishap, and in the presence of continuous stresses.

Responsibility for resilience cannot be outsourced. The University aims to ensure it has necessary attributes and resources to continually assess relationships between its system and environment, recognise emerging hazards, absorb stress consequences and/or disturbance and use adversity as an opportunity for change and improvement.

---

4. SCOPE AND APPLICATION OF THE FRAMEWORK

4.1 Introduction
BCM is an integral part of the University’s approach to effectively managing risk. This framework defines the University BCM methodology and continuity planning process for managing disruption-related risk.

4.2 BCM Policy
The University BCM Framework is underpinned by the University BCM Policy. This Policy defines continuity and recovery principles against which its capability can be audited. The principles encompass elements of:

- Responsibility;
- Strategy and structure;
- Protection;
- Adaptation;
- Performance;
- Learning.

Particular requirements are:

- **Establish** a control environment to link corporate governance, risk management, business planning and operational performance to the University strategic direction (business continuity programme);
- **Invest** time, capital, tools and techniques to ensure BCM is a fully embedded, auditable business management process (business continuity planning);
- Provide senior managers with opportunities to obtain a sound understanding of business continuity management and requisite skills to implement business continuity effectively;
- **Ensure** the framework is sufficiently flexible to meet the challenges of scalability, different University business profiles and various geographic needs coupled with governance, regulatory and legal regimes;
- **Establish** a locus of control to assist others manage events that require information and resource coordination across multiple business functions and/or campuses (Crisis Management Planning); and
- **Uphold** a resilience philosophy in which the University business continuity capability always reflects the needs, technology, structure and culture of its business.

This framework and methodology is based on Standards AS/NZS 5050:2010 Business Continuity – Managing disruption-related risk and ISO 22310 Societal security – Business continuity management systems.

4.3 Objective of the Framework
The aim of this framework is to inform and drive continual, effective, cross-functional, multi-level continuity planning through holistic, integrated risk management practice.
Performance drivers are:

- Structured co-ordination – highly structured co-ordination arrangements ensure that all planning and systems, from the initial business response to recovery and full functionality, are aligned and well understood and communicated, with roles and responsibilities clearly defined and documented;
- Capability building – develop workforce capability and competencies through plans, skills training and role rehearsals, and adequate provision of technical equipment and committed resources;
- Capacity building – build capacity planning dimensions into strategic and operational activities, including escalation processes and systems to manage possible surges in demand;
- Interoperability of plans – ensure interoperability of planning and operational activities taking into account inter and intra-dependencies.

4.4 Roles and Responsibilities
The University Council and Executive Group are accountable for BC and resilience in Griffith University. Ownership of the BCM framework sits with the Vice President (Corporate Services) alongside the current risk management framework.

BCM roles and responsibilities relate to those outlined in the University Risk Management Framework. In addition, each Pro Vice Chancellor is responsible for the sustainability of key critical business functions within their element.

4.5 Communication about BCM
Ongoing BCM communication and consultation with all parties involved is managed through the Risk and Business Continuity Unit, under the authority of the Vice President (Corporate Services).

The Risk and Business Continuity Unit is responsible to facilitate an integrated and collaborative approach to risk and continuity management with core services defined as:

- Policy development and maintenance;
- BCM programme implementation and maintenance;
- Risk and business continuity strategic and operational planning support;
- Internal consultation with University offices to build capability through training, capability exercising, performance monitoring, evaluation and reporting;
- Representation at appropriate forums.
5. BCM PROGRAMME

5.1 Introduction
The BCM programme provides the road map for implementing and navigating through the BC process, and a means for monitoring status and driving continual improvement. The programme lifecycle is outlined in Figure 2.

Figure 2: BCM Lifecycle.  

“Understanding your business” is the professional practice within the BCM lifecycle to review the University in terms of mission, objectives, how it works functionally and the constraints of the environment in which it operates.

This programme provides an auditable quality management approach to:

- Assign responsibilities;
- Establish and implement BCM in the University;
- Monitor, review and continually improve the University continuity performance.

Specific programme deliverables include:

- **Governance**: Policy and standards established and embedded as a management process;
- **Plan**: Threats, vulnerabilities and consequences to mission critical functions and processes are analysed, risk treatment options assessed, and where required pragmatic, achievable business continuity plans developed to suit the nature and scale of the University;
- **Educate, train and equip**: Engaged and empowered staff through education, training and two-way communication;

---

3 Source: Business Continuity Institute
• **Exercise**: BCM established as a normal part of the University business;
• **Evaluate and improve**: High level metrics developed against which programme performance can be monitored, reviewed and continually improved.

The BCM programme will involve the integration of the disciplines of:

• Emergency Management (People and property issues);
• Crisis Management (Corporate issues);
• Business Continuity Planning (Process contingencies);
• Disaster Recovery (IT system and data availability).

### 5.2 Business Continuity Planning Methodology

BCM is about being pragmatic, but also creating a capability in a planned manner. Having a planned business continuity capability denotes a proactive attitude which will enhance the University’s image with students, employees and both internal and external stakeholders.

Additional benefits include improvement in overall organisational efficiency by addressing the issue of complexity, as the BC planning process employs systems thinking to promote a better understanding of the interrelationship between the University core teaching and research functions, the business support/administrative services, resources and critical processes required to ensure their continued viability, and upstream, downstream and third party dependencies.

In undertaking BC planning, determining the cause of a disruptive event is secondary to identifying critical business functions and processes that:

• Have the greatest exposure and susceptibility to interruption;
• The greatest significance to achieving time-sensitive objectives and strategic success.

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

Business Continuity planning for University critical processes will be integrated with emergency management arrangements, the IT disaster recovery planning programme to the extent IT is involved with the process, and its crisis management planning and communication activities. The IT DR programme should be fundamentally driven by the critical business process demands. From these business demands, certain core or common IT infrastructure and data components will be identified that must exist to support all processes.

A BC Plan is owned and developed by the relevant Senior Manager. Each critical process should have its own continuity strategies, which can be invoked individually or en-masse as required, whilst all assumptions made through the planning lifecycle will be captured and validated to ensure appropriate capabilities will exist if/when required.

Senior Managers must ensure the BC Plan is:

• Written and disseminated so various groups of personnel can implement it in a timely manner;
• Specific regarding what conditions should prompt activation of the plan;
• Specific regarding what immediate steps should be taken during a disruption;
• Specific regarding key assets and resources required to support critical processes;
• Flexible to respond to unanticipated hazard/threat scenarios and changing internal conditions;
• Focused on how to get the business up and running if a specific facility, work area or function is disrupted, rather than on the precise nature of the disruption;
- Effective in minimising discontinuity and loss;
- Available in several formats including hard copies with copies kept off-site;
- Integrated into ongoing business planning and system development life cycles.

The key objectives of the BCP are:

- Document critical business processes to be sustained;
- Document resources required to support critical processes;
- Document maximum outage before risk of harm or loss to objectives;
- Document staged recovery times and data points to restore business function;
- Outline alternative accommodation arrangements;
- Document vital records and storage details to support business resumption;
- Establish chain of command, responsibilities and back-up personnel;
- Document notification and escalation procedures.

Committing to a University risk-based BC programme will enhance understanding of disruption-related risk, continuity planning and response management and increase staff vigilance and competency to work around business disruption until full functionality is restored or a new mode of operation implemented. The BC planning process is outlined in Figure 3 and described further below.

Step one in Figure 3 is not explained beyond confirming a management commitment to this process.

Figure 3: BC Planning Process using Risk-Based Approach<sup>4</sup>.

---

<sup>4</sup> Source: HB 221:2004
5.2.1 Step 2: Risk and Vulnerability Analysis

The initial analysis provides the understanding of

- University’s core business functions;
- Critical processes;
- Assets (anything of material value or usefulness);
- Extent of the contribution of each asset;
- Exposure and susceptibility or processes and assets to interruption.

Senior management will:

- Identify threats (hazards) to core business function continuity and the processes, systems, information, people, assets, outsource partners and other resources that support or rely on them;
- Systematically analyse likelihood and consequence of disruption and rate using the consequence ratings in the risk management framework;
- Evaluate which disruption-related risks require treatment; and
- Identify treatments commensurate with BC objectives and in accordance with the University’s risk appetite.

Planning steps for the risk assessment/analysis should include:

- Evaluation of vulnerability; i.e. exposures, susceptibility and effectiveness of existing controls;
- Identification of potential improvements and creation of new measures to mitigate vulnerability, thereby reducing any residual risk to an acceptable level.

If the initial risk analysis does not provide sufficiently reliable information, or if after the initial treatment the residual risk is not tolerable, then a more detailed study called a Business Consequence Analysis (BIA) will be conducted.

5.2.2 Step 3: Business Consequence Analysis

BIA is the process of determining how damaged operations would be over time if assets were not available to support critical business processes and the effect this would have on business functions. A business process describes a set of recurring activities - a flow of information and/or materials that produce an output - something of value for the customer. It is vital to understand the relationship between University core functions, operations, business processes and customers’ level of expectations in order to analyse the consequence of an interruption, and determine which processes are critical for business continuity.

The BIA is aimed at building an understanding of disruptive consequences or potential problems which require treatment and, as such, are likely to exceed routine methods of management or require additional management capability. It identifies the operational (qualitative) and financial (quantitative) consequence of disruption, and forms the basis for the development of viable continuity and recovery strategies to be enacted when necessary to restore operations within required time frames.

The outputs from the initial risk assessment/analysis and the BIA should be consolidated so likelihood of disruption associated overall consequences and mitigation strategies (contingent actions) are recorded in the University enterprise risk register.
5.2.3 **Step 4: Define Response Strategies**
Determination and selection of strategy is based on outputs from the BIA, and built upon the Maximum Acceptable Outage (MAO) identified for each critical process. Senior management will determine appropriate business continuity strategy to:

- Protect University core functions and critical business processes;
- Stabilise, sustain, recover and restore functions, services, critical processes and their dependencies and supporting resources;

Response strategy will be informed by approved time frames for recovery of critical processes (Recovery Time Objectives - RTO). This is the target time for resuming delivery of an operation before MAO is breached and objectives are affected. Where required, strategy will also address the restoration target or Recovery Point Objective (RPO) for the integrity and availability of data (electronic and paper).

When selecting response strategies the following should be considered:

- The type of hazard(s) the group is exposed to;
- Alternate procedures for carrying out the process to completion or to a minimal acceptable level until recovery can be effected;
- Manual processing abilities and related costs;
- Use of insurance (replace rather than salvage);
- 3rd party arrangements, business partnering/dependencies, sector mutual aid;
- Business cycles and peak periods;
- Internal resource capabilities, critical supply chains and vendor management;
- Deciding whether or not an alternative site is required;
- Accessibility of data;
- The option to do nothing – deciding how much the business can afford to lose.

5.2.4 **Step 5: Developing Resource and Interdependency Requirements**
The Business Continuity plan will indicate resource requirements to support critical processes and establish where resources are shared. The types of resources considered shall include, but not be limited to:

- People;
- Information and data;
- Buildings, work environment and associated utilities;
- Facilities, equipment and consumables;
- Information and Communication Technology (ICT) systems;
- Transport and logistics;
- Finance;
- Partners, 3rd party arrangements and suppliers.

5.2.5 **Step 6: Develop Business Continuity Plans**
The BC Plans will set out (as relevant):

- Critical processes to be continued/recovered;
- Defined roles and responsibilities and contact details for people and teams having authority during and following a disruptive event;
- A process for invoking and escalating the response;
- Resources required to support the response;
- A communication strategy;
- Interdependency relationship details;
• Critical supplier/vendor details and alternate arrangements;
• A list of relevant vital records, storage and access details;
• Strategies to manage loss of/interruption to:
  o People;
  o Property;
  o Platforms;
  o Providers (or any combination of the above).

5.2.6 Step 7: Develop a Communication Strategy
A key part of managing any disruptive event is to develop a clear and effective communication and consultation strategy. The strategy must be deployed in a manner that reflects the magnitude of business consequence. Senior management shall establish, implement and maintain procedures to:

• Detect a disruptive event;
• Regularly monitor an event;
• Manage internal communication within the University and receive, document and respond to communication from interested parties;
• Assure availability of the means of communication during an event;
• Facilitate structured communication with emergency responders;
• Record vital information about the event, actions taken and decisions made.

5.2.7 Step 8: Training, Testing and Maintaining Plans

Training
This will ensure what has been developed and documented within the BCP will enable the business unit to sustain critical business processes following a disruptive event.

Education and training are necessary components of the BCM process and require commitment from University personnel involved in planning, response and recovery operations. Some avenues for training include:

• Board and team meetings/planning days;
• Employee orientation;
• Risk management training;
• Specific BC training;
• Emergency evacuation testing.

Training in the creation, implementation, testing and maintenance of BCPs will be organised through the Risk and Business Continuity Unit under the authority of the Vice President (Corporate Services).

Testing
As a critical indicator of success, all BCPs should be tested (rehearsed) and evaluated on a regular basis, results documented and improvements implemented. This will ensure they remain relevant, current and effective. Response and recovery action is to be practiced under simulation conditions in order to:
- Exercise strategies and plans and challenge assumptions;
- Rehearse people with BCM roles and responsibilities.

Exercising of the BC Plan may take various forms including:

- Call tree test – Test currency of listed contact numbers and role knowledge of persons in the tree;
- Desk check test – Review of document in-situ;
- Walk through test – Plan participants walk through the plan procedures in response to a scenario to validate their role knowledge and confirm viability of the plan against business objectives and risk environment.

An explanation of methods and techniques available to test a BCP is outlined in Table 1.

**Maintaining**
A schedule for the ongoing maintenance of the BCP must be established and reported against as part of a quality assurance process. Schedule support will be provided through the Risk and Business Continuity Unit under the authority of the Vice President (Corporate Services).

Table 1 details a recommended methodology.

**Table 1: BCP exercise methods and techniques**

<table>
<thead>
<tr>
<th>Type of Test</th>
<th>Process</th>
<th>Participants</th>
<th>Frequency</th>
<th>Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desk Check</td>
<td>Check the structure and content of the plan</td>
<td>Author of plan</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Walk Through</td>
<td>Discuss the theory of the plan to check that it is usable</td>
<td>Author of plan, Users of the plan</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Simulation</td>
<td>Use the plan to undertake a theoretical response to an incident</td>
<td>Facilitator, Users of the plan, Others as required (e.g. observers)</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Unit Test</td>
<td>Confirm that a recovery procedure or the recovery of a piece of technology works</td>
<td>Users of the procedure or technology, Others as required (e.g. technicians)</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Unit Rehearsal</td>
<td>Practice a recovery procedure or the recovery of a piece of technology, following a script</td>
<td>Users of the procedure or technology, Others as required (e.g. technicians)</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>End-to-End Test</td>
<td>Confirm that the recovery of a complete area of the organization (a business process, product or service or inter-connected technologies) works</td>
<td>Those in the area of the organization, or all those that are required for the business process, product or service, or users of the inter-connected technologies, Others as required (e.g. technicians)</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Full Rehearsal</td>
<td>Practice the recovery of a complete area of the organization, a business process, product or service or inter-connected technologies, following a script</td>
<td>All those in the area of the organization, or all those that are required for the business process, product or service or all the users of the inter-connected technologies, Others as required (e.g. technicians)</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>

5 Good Practice Guidelines 2010
Senior management will take responsibility for ensuring exercises consider cost, complexity and risk and are facilitated at appropriate intervals and after a disruptive event. Figure 4 (below) shows how cost, complexity and risk are interrelated.

Figure 4: BCP exercise cost, complexity and risk\(^6\).

5.2.8 Step 9: Activation and Deployment of Plans
When a disruptive event occurs and results in the activation of BC procedures, senior management and key personnel involved shall undertake a post-event debrief and record the observations and recommendations to inform subsequent action planning.

\(^6\) Good Practice Guidelines 2010
6. LINK BETWEEN BCP, EMERGENCY, CRISIS AND DISASTER RECOVERY PLANNING

6.1 Introduction
The link between BCP, emergency, crisis and disaster recovery planning (Figure 5) is very important. There is a requirement for the University to be able to address any issue of threat at the earliest, most appropriate and most effective opportunity.

Figure 5: Link between BCP, emergency and crisis planning7.

There are a number of phases following a disruptive event that might trigger business continuity plan activation, viz:

- A disruptive event causes a process failure;
- Immediate response including the assessment of the situation and the safety and security of people, equipment and the environment;
- Plan invoked to sustain critical processes and commence phased recovery of operations and
- IT system support to full functionality;
- Should the BCP be ineffective it may be necessary to escalate recovery activity to either the Emergency Response Plan or the Crisis Management Plan - BCP MUST incorporate escalation pathways;
- Plan stand-down following resumption of normal activity.

The response to these phases may occur over a very short or a protracted time, and it is vital that communication is unambiguous and lines of authority are clear.

An ideal escalation path is shown in Figure 6.

---

7 Adapted from Australian National Audit Office (2009)
BCM incorporates emergency management, crisis management and IT disaster recovery planning. A key feature of BCM is clear escalation paths between plans and clear delineation of roles and responsibilities in each level. BCP is concerned with having a robust process that will:

- Allow the University to adequately respond to business disruption to (in the first instance) identified critical processes and collaterally to wider processes within the business unit;
- Better understand uncertainty;
- Understand potential for different types of disruption;
- Plan for future management of disruptions and develop business improvement options to reduce the likelihood and /or cascading consequences of significant future disruption.
7. **FRAMEWORK MAINTENANCE AND ASSURANCE**

The University will conduct internal audits at planned intervals to provide information and assurance on whether:

- The BCM Framework conforms to University requirements, relevant standards and best practice;
- The BCM Programme is effectively implemented and maintained;
- BC plans are properly maintained through:
- Routine training and rehearsing of key personnel,
- Ensuring availability of critical resources,
- Ensuring currency of information, particularly contact lists,
- BC plans are regularly tested to ensure they are adjusted for changes in technology, personnel and risk environment, and they work when deployed;
- The entire BCM process is operating as documented in the BCM Policy.

8. **REPORTING**

The Executive Group shall review the University BCM Framework at planned intervals to ensure its continued suitability. The executive review will consider:

- The status of actions from previous reviews;
- Changes in internal and external issues relevant to the framework;
- Information on BC performance, including trends in:
  - Non-conformities and corrective action strategies,
  - Monitoring and performance measurement results,
  - Audit results,
- Opportunities for continual improvement including:
  - Emerging good practice and guidance,
  - Lessons observed from disruptive events.

9. **RESOURCES**

Tools and templates will be available to support the BC planning process and assist senior managers to:

- Understand what the operational and financial consequences and exposures are to their business function and associated dependencies should a disruptive event occur;
- Be able to define the critical business processes that must be able to continue, more or less uninterrupted should a disruptive event occur;
- Similarly define the priorities for the resumption of the remaining business activities;
- Produce a blueprint of the resource requirements to support process continuity and enable a phased recovery. Resources relate to:
- Staff – include succession planning,
- Space – buildings, work areas,
- Stuff – equipment, infrastructure and information,
- Funding
- Document and register physical assets for insurance purposes;
- Identify the present level of preparedness to deal with a disruptive event should it occur;
- Explore the ‘what ifs’ and implement positive control variables which enable the business function to adapt and change;
• Leverage the capacity of staff to adapt under uncertainty and pressure to give greater operational resilience;
• Remain alert at all times to the threat and implications of a disturbance in all contexts.

BCM tools and templates will be developed and maintained through the Risk and Business Continuity Unit.