Griffith UNIVERSITY

Business Continuity Management and Resilience Framework

Approving authority	University Council
Approval date	3 December 2018
Advisor	Peter Bryant | Vice President (Corporate Services) vpcorporateservices@griffith.edu.au | (07) 373 57343
Next scheduled review	2021
Document URL	http://policies.griffith.edu.au/pdf/Business Continuity Management and Resilience Framework.pdf
TRIM document	2018/0000142
Description	This framework sets out the approach, processes and procedures for managing the University's business continuity and resilience to protect against disruptive events.

Related documents

Business Continuity Management and Resilience Policy
Risk Management Policy
Risk Management Framework
Financial and Performance Management Standard 2009
Financial Accountability Act 2009
Health and Safety Policy
Emergency Management Plan
Crisis Management Plan

1. INTRODUCTION

Business Continuity Management (BCM) is an integral part of the University's approach to effectively managing risk. This framework defines the BCM methodology and continuity planning process for managing disruption-related risk.

The BCM Framework is underpinned by the Business Continuity and Resilience Policy. The Policy defines continuity and recovery principles against which its capability can be audited.

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.

2. PURPOSE OF THE BUSINESS CONTINUITY MANAGEMENT AND RESILIENCE FRAMEWORK

The purpose of this framework is to inform and drive continual, effective, cross-functional, multi-level continuity planning through holistic, integrated risk management practice in the following ways:

- 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;
- Assist and 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.

3. WHAT IS BUSINESS CONTINUITY MANAGEMENT?

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

Disruption refers to an outage which has a time and business consequence dimension but does not include 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.

Disruption-related risks may be infrequent, but could have severe consequences for critical services, which are not able to be resolved by routine management. Disruption-related risks include physical and non-physical events, such as, natural disasters, pandemics, significant loss of utilities, financial crises, accidents, and incidents that threaten our reputation.

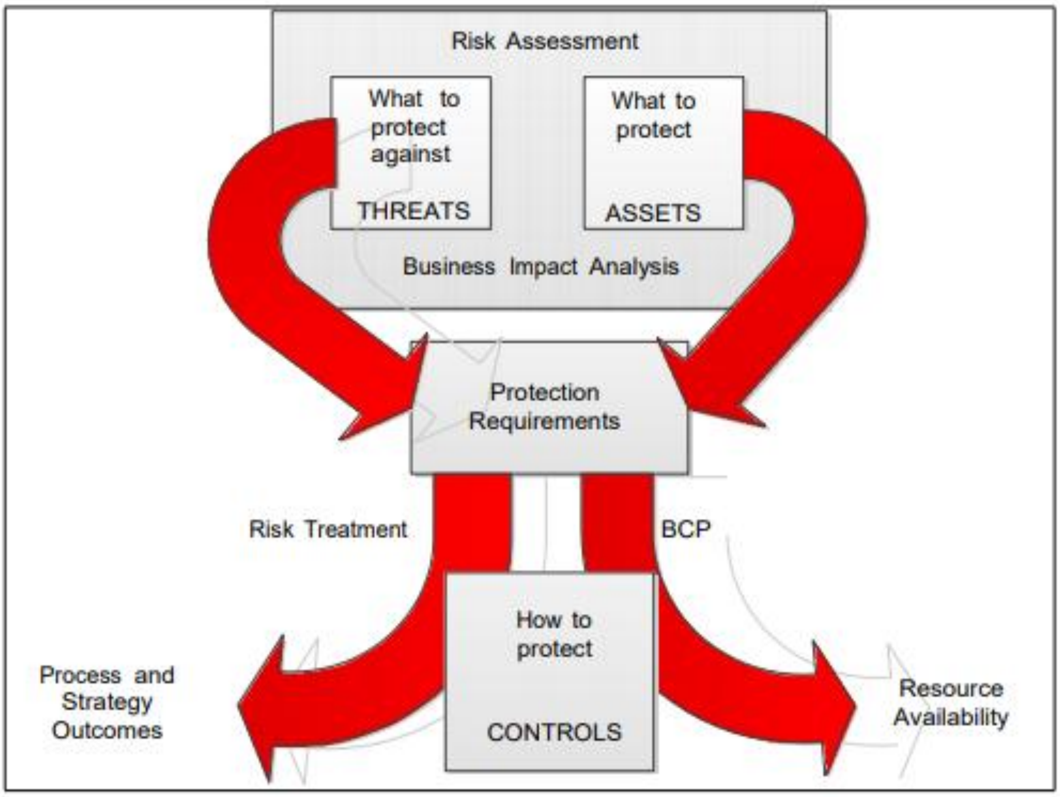
BCM is the development, implementation and maintenance of policies, strategies and programs to assist the University to manage a business disruption event, as well as build resilience. It is the capability that assists in preventing, preparing for, responding to, managing and recovering from the impacts of a business disruption event.

BCM is an application of risk management, an integral component of sound corporate governance and an important aspect of emergency preparedness and operational resilience. An 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.

The objectives of BCM are to:

- Keep people safe;
- Reduce the University’s 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

The key functional elements of BCM are outlined below.



4. THE BUSINESS CONTINUITY APPROACH

Business Continuity Planning (BCP) is a function within BCM. The approach for BC is a continuous planning and preparing process of identifying hazards and University vulnerabilities, the likelihood of disruption, potential consequence on time-sensitive objectives and strategic success, existing control effectiveness and options 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 approach are:

- **Understand the business** - 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, assurance that if the worst happens the University has the capacity to recover quickly, safely and as cost effectively as possible.

The BCM approach will also 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).

Committing to a University risk-based BC approach 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.

5. THE BUSINESS CONTINUITY PROCESS

The illustration below demonstrates the roadmap for the business continuity process

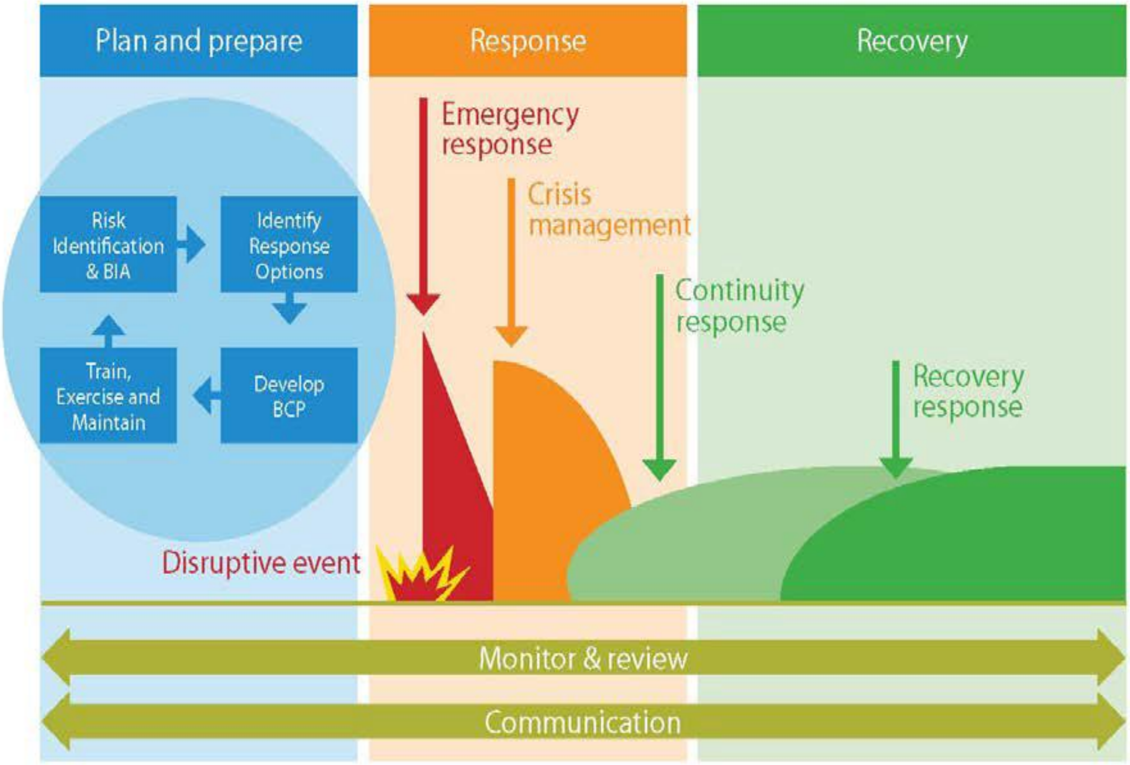


Figure 1: The relationship between the activities in managing disruption-related risk
Source: Adapted from Marsh & McLennan Companies

Step 1: Risk Identification and Business Impact Analysis

Risk Identification

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 the 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 Impact Analysis (BIA) will be conducted.

Business Impact Analysis (BIA)

BIA is the process of determining how operations would impacted 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 (students and other key stakeholders). It is vital to understand the relationship between University core functions, operations, business processes and customers’ level of expectations 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.

Step 2: Identify and Define Response Options

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 option and strategy to:

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

Response options and 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 options and 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);
- Third party arrangements, business partnering/dependencies, sector mutual aid;
- Business cycles and peak periods;
- Internal resource capabilities, critical supply chains and vendor management;
- Deciding whether an alternative site is required;
- Accessibility of data;
- The option to do nothing – deciding how much the business can afford to lose.

Step 3: Develop Business Continuity Plans

A BC Plan is owned and developed by the relevant Senior Manager. Each critical process should have its own continuity strategy, 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.

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:
    - People;
    - Property;
    - Systems
    - Providers (or any combination of the above).

Step 4: 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.

Step 5: Training, Testing and Maintaining Plans

Training

Training 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 Offices of Audit, Risk and Compliance, Campus Life and Digital Solutions, 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 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 the Table below

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 Office of Audit, Risk and Compliance under the authority of the Vice President (Corporate Services).

The Table below details a recommended methodology.

Table 1: BCP exercise methods and techniques

Type of Test	Process	Participants	Timeframe
Desk Check	Check the Structure and content of the plan	Author of the Plan	Annually
Walk Through	Discuss the theory of the plan to check that it is usable	Author of the Plan Users of the Plan	Annually
Simulation	Use the plan to simulate a theoretical response to an incident	Facilitators Users of the Plan Others as required (e.g. observers)	Bi-Annually
Unit Text	Confirm that a recovery procedure or the recovery of a piece of technology works	Users of the procedure or technology Others as required (e.g. technicians)	Bi-Annually
Unit Rehearsal	Practice a recovery procedure or the recovery of a piece of technology following a script	Users of the procedure or technology Others as required (e.g. technicians)	Bi-Annually
End-to-end	Confirm that the recovery of a complete area of the organisation (business process, product or service or inter connected technologies) works	Those in the area of the organisation or those that are required for the business process, product or service, or users of the inter-connected technologies Others as required (e.g. technicians)	Annually
Full Rehearsal	Practice the recovery of a complete area of the organisation business process, product or service or inter connected technologies, following a script	Those in the area of the organisation or those that are required for the business process, product or service, or users of the inter-connected technologies Others as required (e.g. technicians)	Bi-Annually

Senior management will, where applicable, take responsibility for ensuring exercises consider cost, complexity and risk and are facilitated at appropriate intervals and after a disruptive event.

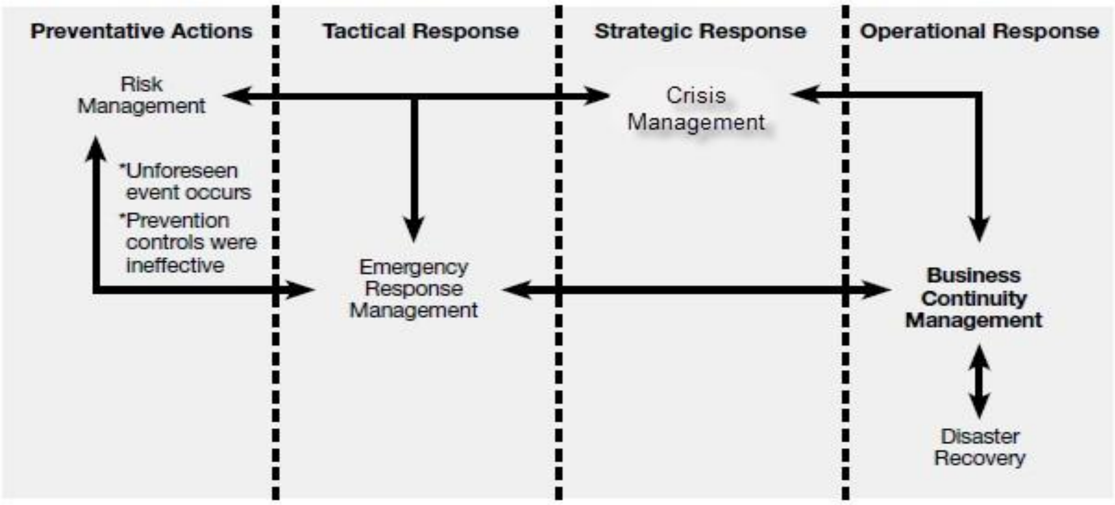
Step 6: Activation and Deployment of Plans

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. LINK BETWEEN BCP, EMERGENCY, CRISIS AND DISASTER RECOVERY PLANNING

The link between BCP, emergency, crisis and disaster recovery planning are very important. There is a requirement for the University to be able to address any issue of threat at the earliest, most appropriate and in an effective manner.

The illustration below demonstrates the links:



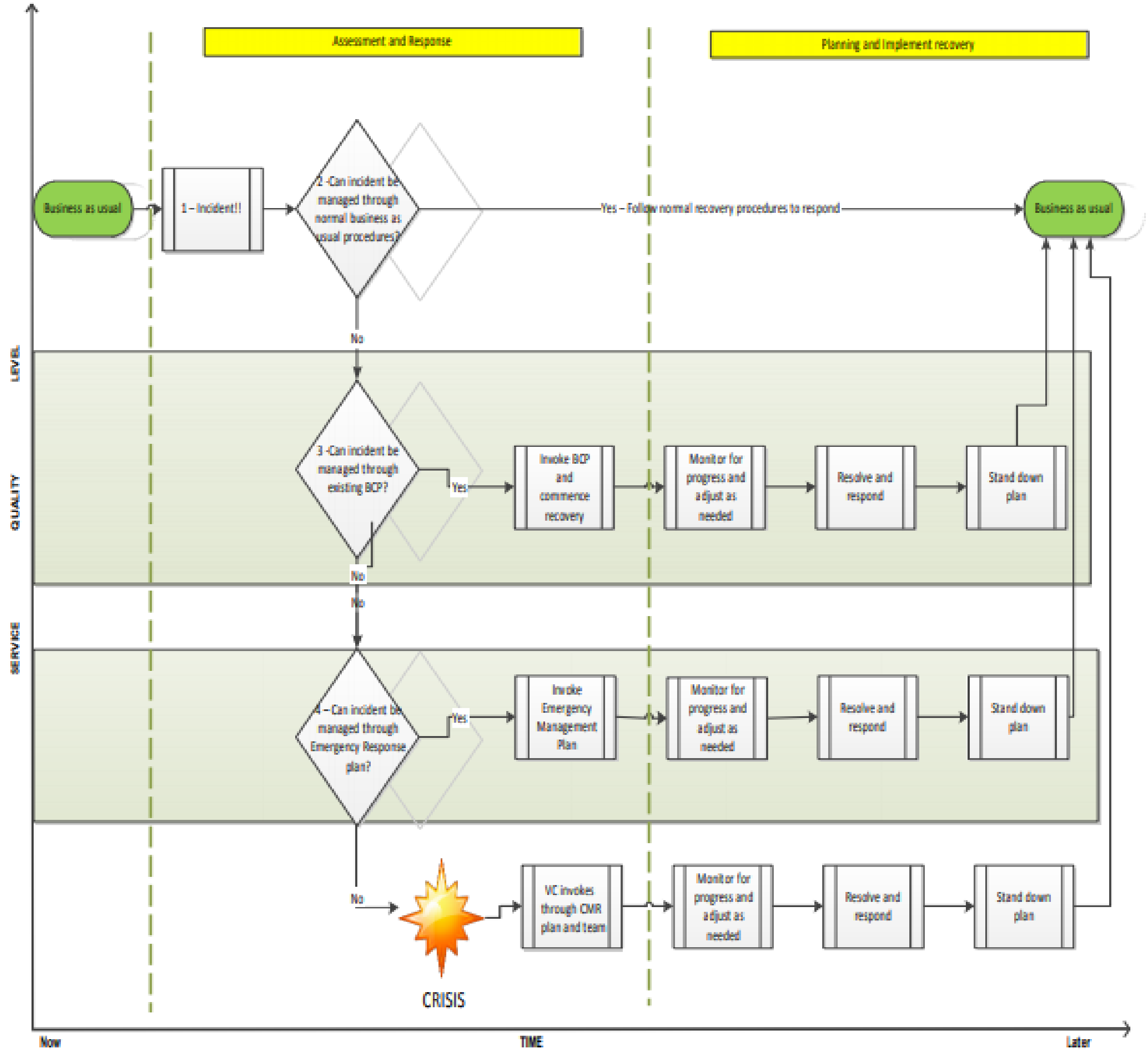
There are a number of phases following a disruptive event that might trigger BCP activation, viz:

- A disruptive event causes a process failure;
- Immediate response including the assessment of the situation and the safety and security of people, assets 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 the illustration below.

Figure 6: BCM Escalation Path


Assessment and Response
Planning and Implement recovery
Business as usual
1 – Incident!!
2 -Can incident be managed through normal business as usual procedures?
Yes – Follow normal recovery procedures to respond
Business as usual
No
3 -Can incident be managed through existing BCP?
Yes
Invoke BCP and commence recovery
Monitor for progress and adjust as needed
Resolve and respond
Stand down plan
No
No
4 – Can incident be managed through Emergency Response plan?
Yes
Invoke Emergency Management Plan
Monitor for progress and adjust as needed
Resolve and respond
Stand down plan
No
CRISIS
VC invokes through CMR plan and team
Monitor for progress and adjust as needed
Resolve and respond
Stand down plan
LEVEL
QUALITY
SERVICE
Now
TIME
Later

7. ROLES AND RESPONSIBILITIES

The University Council and Executive Group are accountable for BCM and resilience. 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, the Executive Group, is responsible for the sustainability of key critical business functions within their Groups or Element.

8. COMMUNICATION

Ongoing BCM communication and consultation with all parties involved is managed through the Director Audit, Risk and Compliance and the and the Manager Risk and Business Continuity Planning, under the authority of the Vice President (Corporate Services).

The Manager Risk and Business Continuity Planning is responsible for facilitating 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; and
- Representation at appropriate forums.

9. 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 processes are effectively implemented and maintained;
- BCPs are properly maintained through:
  - Routine training and rehearsing of key personnel,
  - Ensuring availability of critical resources,
  - Ensuring currency of information, particularly contact lists,
- BCPs are regularly tested to ensure they are adjusted for changes in technology, personnel and risk environment, and they work when deployed;

GLOSSARY OF TERMS

Term	Definition
Business Continuity (BC)	A state of continued, uninterrupted operation of a business in all contexts.
Business Continuity Management (BCM)	"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.
Business Continuity Management Process	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 Plan (BCP)	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.
Business Impact Analysis (BIA)	The process of analysing business functions and the effect that a business disruption might have upon them. The BIA provides a level of analysis to examine in detail any consequences that may exceed routine management capability.
Communication and Consultation	"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)
Control	Any measure or action that modifies or regulates risk. Controls include any policy, procedure, practice, process, technology, technique, method, or device that modifies or regulates risk. Risk treatments become controls, or modify existing controls, once they are implemented. (AS/NSS ISO 31000:2018). Business Continuity controls ensure an uninterrupted availability of key business resources that support the continuation of key or crucial business processes and objectives.
Consequence	Outcome of an event and has an effect on objectives. A single event can generate a range of consequences which can have both positive and negative effects on objectives. Initial consequences can also escalate through cascading and cumulative effects. (AS/NSS ISO 31000:2018)

Corporate Governance	Primarily concerned with, but not limited to: • Effectiveness and efficiency of operations; • Compliance with laws and regulations; • Vulnerability of the organisation and safeguarding of assets. 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.
University Council	The Council of Griffith University.
Crisis	Any event that is, or might lead to, an unstable or dangerous situation affecting an individual or group.
Disruption- related risk	University consequences of being unable to remain operational. Refers to how quickly or severely an outage could affect achievement of University time sensitive objectives. Disruption related risk management is a particular application of risk management.
Event	An incident or situation, which occurs in a particular place during a particular interval of time.
Hazard	A source of potential harm or a situation with a potential to cause loss. The words ‘threats’ and ‘hazards’ are often interchangeable.
Likelihood	Used as a qualitative description of probability or frequency of a risk occurring.
Loss	Any negative consequence, financial or otherwise. Can be differentiated as follows; • Maximum foreseeable loss- highest possible loss after considering controls • Maximum possible loss – highest possible loss without considering controls
Maximum Acceptable Outage (MAO)	The duration after which the University’s viability will be threatened if a service or function cannot be resumed.
Mitigation	Involves pre-empting a challenge and taking steps to avoid the threat or limit any negative consequence.
Probability	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.
Recovery	“Steps taken to resume the business within an acceptable timeframe following a disruption.” (Business Continuity Institute)
Recovery Point Objective (RPO)	“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.” 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)
Recovery Time Objective (RTO)	“The target time for resuming the delivery of a product or service to an acceptable level following its disruption.” (Business Continuity Institute)
Residual Risk	The remaining risk after management has taken action to alter the risk’s likelihood or impact.

Resilience	The University’s ability to achieve its immediate objectives in uncertain and non-routine times.
Risk	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.
Risk Analysis	A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.
Risk Appetite	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: • Spatial distribution • Temporal distribution • Intensity (how big/fast/powerful)
Risk Assessment	The overall process of risk analysis and risk evaluation.
Enterprise Risk Management Framework	The totality of the structures, methodology, procedures and definitions that the University has chosen to use to implement its Risk Management Processes.
Risk Register	The means by which the University elects to manage or treat the individual risks. he 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.
Stakeholders	Those people and organisations who may affect, be affected by, or perceive themselves to be affected by, a decision or activity.
Vulnerability	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.

2. Glossary of Acronyms

BC	Business Continuity
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
IT DR	Information Technology Disaster Recovery
MAO	Maximum Acceptable Outage
RPO	Recovery Point Objective
RTO	Recovery Time Objective