



# JCU Business Continuity Management Plan





7.4.2 Desk top exercise.....24

7.4.3 Simulation.....24

7.4.4 Real Time exercise.....25

7.5 Developing a Test Exercise or Scenario.....25

7.5.1 Outcomes of the test exercise.....26

7.6 Maintenance.....26

7.6.1 Process.....27

7.7 Review.....27

8. Definitions.....29

List of Appendices

Appendix A- BIA Template for Services Register .....31

Appendix B- BIA Template for Impact Definitions.....32

Appendix C- BIA Template for Services Impact .....33

Appendix D- .E-21.6(D)35.3(e).i.....0.56(n)]TJ 0 Tc 0 Tw (i)Tj -0.026  
33

3205157.13.....n.2(Tj-feTs(52.)Tj2.4(.-)s).C.....333333



## 1. Business Continuity Management

### 1.1 What is Business Continuity?

Business Continuity is defined in ISO 22301:2012 Societal Security – business continuity management systems – Guidelines, as:

“The capability of an organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident”.

Adapted to the University context, the definition above can be modified to read:

“The capability of the University to continue to deliver education and research and carry out activities at acceptable predefined levels following a disruptive incident”.

Business Continuity Management (BCM) at JCU is the overall management process that identifies potential threats to the University and the impacts to University operations from those threats, if realised.

BCM also provides a framework for building University resilience. Resilience is widely defined as the ability of an organisation to absorb, respond to and recover from disruptions (BCG:2013). Thus, BC can enhance the capability to respond effectively to business interruption and safeguard the interests of the University’s key stakeholders, reputation and value creating activities and services. Furthermore, by focusing on the impact of disruption rather than the cause, business continuity identifies those activities on which the organisation depends for its survival, and enables the organisation to determine what is required to continue to meet its obligations (ISO 22313:2012).

An organization with appropriate business continuity in place can also take advantage of opportunities that might otherwise be judged to be too high risk, thus BCM can influence risk appetite.

### 1.2 Business Continuity and Risk Management

A high-level assessment of the threats to the University’s strategic objectives has been undertaken as part of the University’s business planning process. This takes the form of the University Level Risk Assessment. Further Divisional risk assessments are also undertaken. The outputs of these activities inform the BCM programme scope.

As part of the University BCM programme, a Business Impact Analysis (BIA) is undertaken. One of the deliverables from the BIA is an understanding of the activities undertaken by the University that are the most urgent. These are the activities that would impact the University the most if they were disrupted for a defined period of time.

The BCM programme identifies and implements strategies to enable these activities to be recovered before the impact of their disruption becomes intolerable. Measures are identified which can be put in place to reduce the chances of such activities being disrupted and the University also quantifies the resulting impact.

Risk assessments are undertaken as part of a BCM programme. These are usually at an operational level as they are concerned with the disruption of activities. They complement risk assessments undertaken at the enterprise level such as the University Level Risk Assessment (ULRA). The overlap between BC and Risk Management provides the University with the opportunity to strengthen its resilience when the management of the two disciplines is coordinated effectively and aligned. Thus, BC fits into the risk management framework that is built around ISO 31000:2009.





## 2. BC Policy and Programme Management

The BC policy is a high level document, approved by University Council, where the commitment to BC is established for communicating throughout the University. It sets out the scope and governance of the BCM programme and reflects the reasons why BCM is implemented.

The policy also identifies the principles to which the University aspires and against which performance can be monitored.

The scope of the BCM programme has been determined before any other stages of the BCM Lifecycle. The University's implementation of BCM is based on key University processes that are essential to the following:

- x Delivery of teaching content
- x The function of student learning methods and assessment tools
- x Conduct of research
- x Management of corporate data and records
- x Compliance with legislative requirements
- x Protection of University reputation

A form of review is carried out at least once every 12 months (refer Sec. 7.7). However, certain information that becomes available will prompt re-examination of the scope:

- x Revision of a BIA that identified substantive changes in processes and priorities; or
- x A significant change in one or more of the following:

- The University's risk appetite (i.e. ~~ES&S (s) 7.0 (2) (b) 13 (a) (2) (1) (5) 7 (a) 5 20 11 1 200~~



## 2.1 Roles and Responsibilities

Given the scale of the University and scope of activities, a suitable Business Continuity Function

Owner (BCFO) Bis-18.91() TJ 00.011 Tc 0.011 Tw 10932 0 Td ((de)-11(i)-16.23g)-13.2(n)aid [TJ 00.0162Tw 1



## 2.4 BC Documentation

BCM Programme documentation has three purposes:

- x To enable a prompt and effective response to an incident;
- x To help manage the BCM programme effectively; and
- x To demonstrate the effective management of the programme

Each business unit is responsible for updating their business continuity documentation. Those responsible for maintaining plans must update their documentation. This also promotes ownership of the process.

The following records management principals need to be followed for all business continuity documentation:

- x All documentation needs to be current. Documents are to be reviewed at 12-monthly intervals to update information, or earlier as changes dictate;
- x Documentation needs to be accessible to all business unit staff who may need to use it for carrying out key organisational processes;
- x All documentation needs be created and maintained in accordance with the University Records Management Policy; and
- x A back-up of all current documentation needs be stored in a manor appropriate to the business unit, which is accessible to the business unit when the University corporate records management system is unavailable.

## 3. Embedding Business Continuity

### 3.1 General

Embedding Business Continuity is an ongoing activity, arising from the BC Policy and BC programme management stage of the BCM Lifecycle. Embedding BC seeks to integrate BC into day-to-day University activities in the same way as risk management or health and safety disciplines.

The University acknowledges that responsibility for BC must be shared across all Divisions in order to be successful. The successful establishment of BC within the University depends on its integration with strategic and day-to-day management, as well as its alignment with institutional priorities.

In developing a culture of BC awareness the University addresses:

- x Barriers to embedding BC. For instance, dealing with attitudes of “we can cope” or “it will never happen here”, if such attitudes are present;
- x The willingness of individuals to undertake BC related tasks, such as maintaining plans, in addition to their normal roles;
- x The assessment of BC related activities of suppliers in determining supplier arrangements or other contractual matters;
- x The inclusion of BC related concepts in planning and decision-making;
- x The performance of staff and management during an incident; and
- x The willingness of staff to take responsibility for risk mitigation and incident response

The culture of the University with respect to BC (and more generally) is influenced by the “Tone at the Top”, that is, the JCU University Council, committees of Council, University Executive (UE) and Vice Chancellor’s Advisory Committee (VCAC).





The University demonstrates leadership for embedding its BCM programme through:

x





Figure 2 : Illustration of business continuity being effective for sudden disruption (excerpt from ISO22313:2012). No particular timescales are implied by the relative distance between the stages depicted in the diagram.

The recovery time objective (RTO) is the period of time following an incident within which a product or an activity must be resumed, or resources must be recovered (ISO 22301:2012).

Note: The RTO must be less than the MAO by an amount which takes University risk appetite into account.

The Recovery Point Objective (RPO) is the point to which information used in an activity must be restored to enable the activity to operate on resumption (can also be referred to as “maximum data loss”) (ISO 22301:2012).

The minimum business continuity objective (MBCO) is a minimum level of service that is acceptable to the University to achieve its business objectives during a disruption (ISO 22301:2012). The RPO will guide the MBCO calculation.

The MBCO level may vary depending on the nature of the service/activity. The MBCO is designed to be achieved at a specific time after a disruption. It may be appropriate to set several MBCOs for different times after an incident and for each service/activity covered in the BCM programme scope.

#### 4.2 BIA Process

The BIA is less focused on the likelihood of incidents occurring and therefore has a different emphasis compared to a risk assessment used to identify threats that can cause disruption. The outputs from the risk assessment (ULRA or Divisional) feed into the BIA.

The University’s BIA analysis framework combines the tasks of strategic, tactical and to a lesser extent operational to create a more streamline approach, initially. The framework is used to clarify the BCM programme scope. The process includes:

- x Deciding the terms of reference and draft scope of the BIA;



x







operation after an incident. Suitable where the







## 6. Business Continuity Plans (Implementation)

### 6.1 General

Implementation is the stage of the BCM Lifecycle that executes the agreed strategies and tactics through the process of developing the Business Continuity Plan (BCP).

The aim is to identify and document the priorities, procedures, responsibilities and resources to assist the University in managing a disruptive incident, while implementing continuity and recovery strategies to a pre-determined level of service.

Business Continuity Plans are created for any level of the University and is not necessarily a single overarching document. BCPs are developed for particular locations and activities/services (e.g. ICT Disaster Recovery Plan).

### 6.2 BCP Methods

The scale and complexity of the University is significant with two campuses in Australia, located in Townsville and Cairns with additional regional sites (e.g. Mackay, Mt Isa, Thursday Is. etc.) and an overseas campus in Singapore.



### 6.3 Developing a BCP

The key steps in developing a plan include:

- x Appoint an owner/sponsor for the plan (e.g. BCFO);
- x Define the objectives and scope;
- x Develop and approve a plan development process;
- x Create a planning team (2-4 people);
- x Agree the responsibilities of the response team and their relationship with other plans and response teams (strategic, tactical and operational);
- x Create a response team having the required skills;
- x Decide the structure, format, components and content of the plan;
- x Determine the strategies, such as alternative locations, on which the plan will be



- x Apply the structure, format, components and content of the plans utilising the BCP template to maintain consistency across the University; and

A tactical plan includes detailed procedures for the team to:

- x Promptly respond to activation;
- x Assess information and make decisions (Go/No Go);
- x Mobilise the teams and invoke resources;
- x Initiate response procedures and recovery activities;



The same steps as those outlined in Sec. 5.3 above can be applied here. Particular focus is on documenting connections with the tactical level plans and between different operational plans. Business units are to nominate individuals to fulfil key roles within their plans.

Plans must include instructions regarding:

- x Staff welfare;
- x Access to and use of facilities;
- x Resumption of business unit activities within agreed recovery time objective levels;
- x Liaison with IT service continuity teams; and
- x Mobilisation of teams and invocation of resources required for recovery purposes.

The above plans must include, as relevant, the following types of procedures and information, such as:

- x Building evacuation and evacuation points (including alternate or off-site);
- x Emergency services liaison;
- x Bomb threat procedure;
- x Redeployment of staff and visitors;
- x Contracted assistance;
- x Escalation procedures;
- x HR and welfare issues;
- x Health and safety liabilities;
- x Procedures for accounting for staff;
- x Procedures for contacting staff;
- x Counselling and rehabilitation resources;
- x Initial response on activation;
- x Contacting team members;
- x Resumption plan for each activity

## 6.6 Communications

The University's strategic level plan addresses how it manages communication with the media, and all plans generally include reference to the University's media strategy and instructions to staff on what to do if approached by the media.

Plans also contain information on what actions the University staff must take if they are involved in an incident which has, or is likely to attract media attention and whom to inform at the University, if contacted by the media.

Media response and communications is handled by specialists in the Chief of Staff Office. The Head of Media and Communications has accountabilities to (but not limited to):

- x Provide strategic and practical media advice to the University's Senior Management Group including but not limited to communications in times of crisis or other incident management, to develop specific strategic and tactical media campaigns for their respective areas of expertise and responsibility
- x Develop and support internal communications strategies and mechanisms, providing advice and training where appropriate to staff on engaging with and presenting news events and stories
- x Develop and maintain professional relationships and effective two-way communication between the media industry and members of the University community





## 7.4 Methods

The types of exercises undertaken by the University are:

### 7.4.1 Discussion-based exercises

- a. Cost effective and the least time consuming of exercise types
- b. Involve commonly structured events where participants explore relevant issues and walk through plans in an unpressurised environment.
- c. Focus on a specific area for improvement identified with the aim of finding a possible solution

### 7.4.2 Desk top exercises

- a. Used where discussion is based on a relevant scenario with a time line which may run in 'real time' or may include different phases of a scenario to be tested (e.g. media response).
- b.



- x Facilitator;
- x



An important part of the BCM Lifecycle is to manage BCM documentation. Maintenance ensures BCM documentation is kept up to date and that current and relevant documentation is distributed to relevant sections of the University.

Maintenance activities are identified through:

- x Lessons learned from BCM testing;
- x Changes in the internal and external environment in which the University operates;
- x Process reviews or internal audit;
- x A real incident, when lessons learned can be incorporated; and
- x Updated or changed BIA outputs hrw





1. Percentage of plans maintained by the scheduled date
2. No. of substantive changes identified from BC maintenance activities (substantive means changes resulting in a training need or awareness campaign)
3. % training completed against a training plan (established from review outcomes)
4. % BIA completion against BCM programme scope (12 BIAs identified within scope and 4 complete = 33% vs. target of 50% in 12 month period) until completed

## 7.7 Review

The purpose of Review is to evaluate the BCM programme as a whole, to identify improvements to both the organisation's implementation of the BCM lifecycle and level of resilience.

There are five basic types of review undertaken by the University:

- x Audit (internal and external) – a formal independent review process that incorporates

Table 3: BCM Programme Assurance

Assurance function	Annual	2-yearly	3-yearly
Internal Audit (BCM component only)		X	9
Self-Assessment (Division based)	9		
Quality Assurance	X	X	9
Performance Appraisal	9		
Supplier Performance	X	X	9

The 'X' denotes higher frequency depending on triggers such as 1) trends in KRIs; 2) disruptive incidents; and 3)





## Appendix A – Services Register

Completed by:

Date last reviewed: xx/xx/xx

Ref	Name of product or service	Critical Activity What are the main activities required to deliver the product or service
-----	----------------------------	--



## Appendix B – Impact Definitions

Insignificant	Incident including first aid, workplace hazard contained immediately and no ongoing safety risk impact. No known similar risk within University.	Insignificant	one off loss of <\$1m	Insignificant	Minor technical breach of standards	Insignificant	inability to deliver face to face courses < 2 days Minor academic indiscretions dealt with according to normal procedures
Minor	Incident including medical treatment, near miss, impacts a minor part of University with minor works <\$100k	Minor	one off loss of between \$1m & \$5m	Minor	Minor breach of regulations or standards	Minor	inability to deliver face to face courses between 2 & 7 days One off instances of minor misconduct dealt with according to normal procedures
Moderate	Lost time injury (< 6 months), finding, ISOS combined extreme/high risk, impacts a moderate to substantial part of University with moderate works between \$100-\$250k	Moderate	one off loss of between \$5m & \$20m	Moderate	One off breach of legal or contractual arrangements requiring legal or regulatory intervention	Moderate	inability to deliver face to face courses between 1 & 4 weeks; Loss of voluntary accreditation of single course; localised fraud or misconduct in academic activities
Major	Single fatality or significant lost time injury (> 6 months), notifiable event, finding, notice, suspension of work impacts a substantial part or whole of University with major works between >\$250-\$500k.	Major	one off loss of between \$20m & \$50m	Major	One off serious successful prosecution or adverse findings, breach of significant contractual arrangement, statutory intervention due to breach of legislation	Major	inability to deliver face to face courses > 4 weeks

## Appendix C – Service /Activity Impact Assessment

Name of Product or Service \_\_\_\_\_

	Impact	Time					Justification
		4 HRS	1 day	2 days	1 week	1 month	
WHS	No Impact						
	Minor	x					
	Moderate						
	Major						
	Critical						

	Impact	Time					Justification
		4 hrs	1 day	2 DAYS	1 week	1 month	
REPUTATION	No Impact						
	Minor						
	Moderate						
	Major			x			
	Critical						

	Impact	Time					Justification
		4 hrs	1 day	2 days	1 WEEK	1 month	
PEOPLE	No Impact						
	Minor						
	Moderate						
	Major				x		
	Critical						

	Impact	Time					Justification
		4 hrs	1 DAY	2 days	1 week	1 month	
FINANCE	No Impact						
	Minor						
	Moderate						
	Major		x				
	Critical						

	Impact	Time					Justification
		4 hrs	1 day	2 days	1 week	1 MONTH	
LEGAL	No Impact						
	Minor						
	Moderate						
	Major						
	Critical					x	

	Impact	Time					Justification
		4 hrs	1 day	2 DAYS	1 week	1 month	
LEARNING & TEACHING	No Impact						
	Minor						
	Moderate						
	Major			x			
	Critical						

	Impact	Time					Justification
		4 HRS	1 day	2 days	1 week	1 month	
RESEARCH	No Impact						
	Minor						
	Moderate						
	Major	x					
	Critical						

Maximum Acceptable Outage	Recovery Time Objective
---------------------------	-------------------------

Unacceptable level of impact		
Work Health and Safety	No Impact	
	Minor	X
	Moderate	
	Major	
	Critical	
Reputation	No Impact	
	Minor	
	Moderate	
	Major	X
	Critical	
People	No Impact	
	Minor	
	Moderate	
	Major	X
	Critical	
Financial	No Impact	
	Minor	
	Moderate	
	Major	X
	Critical	
Compliance and Liability	No Impact	
	Minor	
	Moderate	
	Major	X
	Critical	
Learning and Teaching	No Impact	
	Minor	
	Moderate	
	Major	X
	Critical	
Research	No Impact	
	Minor	
	Moderate	
	Major	X
	Critical	

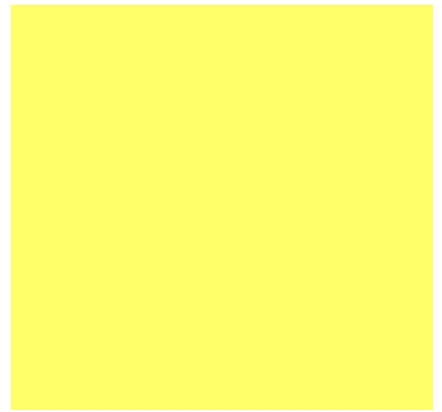
The Maximum Acceptable Outage (MAO) is the maximum period of time the University can tolerate a disruption causing or resulting in impact to the following:

{ t, ^  
 { Z % μ š š } v  
 { W } % o  
 { & ] v v  
 { > P o  
 { > CE v ] v P v d Z ] v P  
 { Z • CE Z

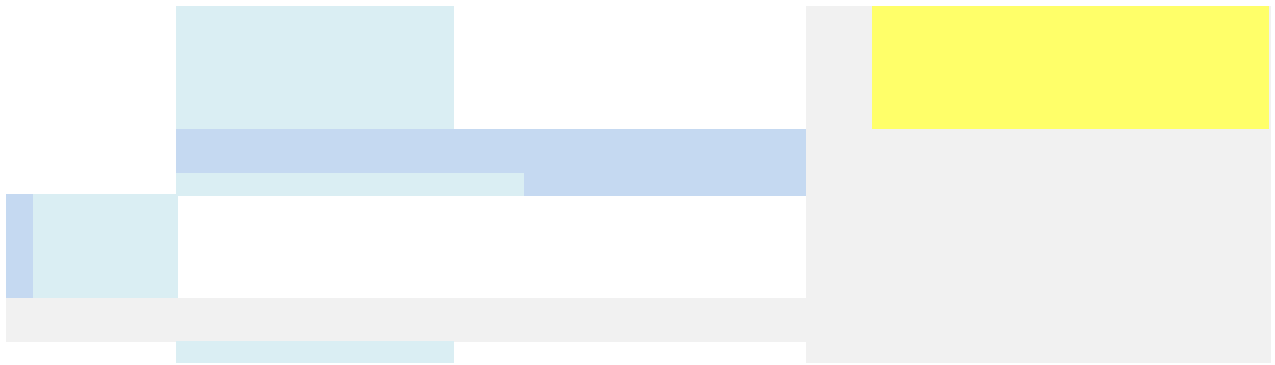
Key University activities/services with a Maximum Acceptable Outage of X period (e.g. 2 days or less) will necessitate a risk assessment to reduce the impact and likelihood of disruption.

## Appendix D – Supplier Assessment

	4 hrs	



Appendix E – ICT Applications Assessment







## Appendix F – Continuity Resource Requirements

Time	Insert the minimum number of resources you would require over time in order to continue your products and/or services within their recovery time objective									
	Building	Staff	Mac	PC	IT applications	Laptop	VPN	Desk phone	Suppliers	Insert resource
4 hours										X
1 day										X
2 days										X
1 week										X
1 month										X

Æ u % o • } ( } š Z œ œ • } μ œ • Ç } μ u Ç Á ] • Z š } ] v o μ W Á } œ l u } ] o U % œ ] v š œ U • v v œ U Z C



## Appendix G – Self Assessment Questionnaire

Business Continuity Management Self - Assessment Questionnaire	
Period of Assessment:	
Division:	Date:
College/Directorate:	Completed by:
Business Unit / Function:	Position Name:

Ref. No.	Area of Assessment / Questions	Score (Y, M, P or N)	Comments
<b>Responsibility and Ownership</b>			
RO1	The DVC, Director or Dean is accountable for business continuity management for the business unit, subject to this self-assessment		
RO2	There is a documented management structure in place at Divisional level, which includes the appointment of business continuity function owner(s) (e.g. 1 per College). The structure addresses each business function/service with clearly defined roles and		

Ref. No.	Area of Assessment / Questions	Score	Comments
<b>Review</b>			
R1	All plans undergo a complete review involving reviewing BC activities against the BCM Lifecycle, revisiting risk assessment and recovery strategies for critical activities and services		
R2	Details on all people involved in an invocation, and the invocation processes are reviewed for key internal/external incident response and recovery providers, (i.e., University, Divisional or Business Unit, on-campus and off-campus)		
R3	A process is in place to ensure plans and response teams are reviewed for composition and skills: <ul style="list-style-type: none"> <li>a) following test exercises where deficiencies are identified</li> <li>b) following incidents including near-misses</li> <li>c) following changes to BIA</li> </ul>		
<b>Testing and Incidents</b>			
T1	A documented annual testing programme is in operation and tests plans (BCPs) at the appropriate level (strategic, tactical, operational)		
T2	The annual testing programme covers a representative selection of business-critical units and processes, and tests the following components against RTO/RPO, MAO and resources		

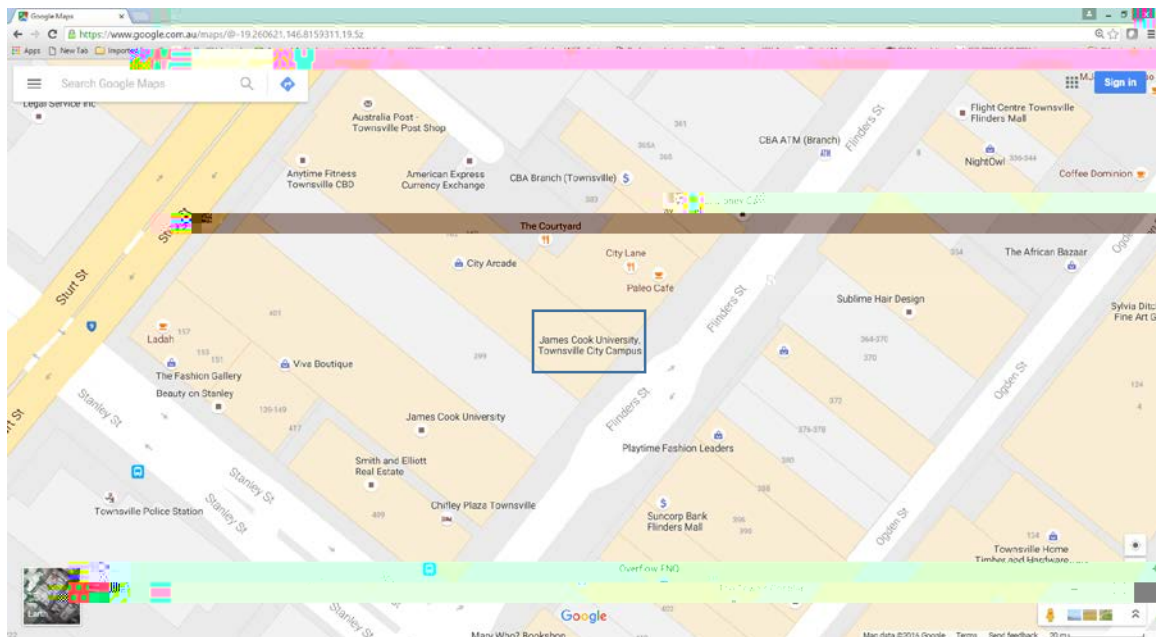




## JCU Townsville City campus and street map



## 383 Flinders St





JCU Cairns