JCU Business Continuity

Management Plan

List of Appendices

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.

Ultimately, BC must be thought of in terms of "what business consequences need to be managed" and not by "what has happened" (e.g. damage to premises, failure of technology, etc).

1.3 Business Continuity and Corporate Governance

BC contributes to effective corporate governance as it helps parties to ask and review key questions that address the following, including any changes to:

- The resilience of the University's operating model;
- Key value-creating services and activities;
- Key dependencies – priority assets and processes;
- How the University would respond to a loss of, or threat to priority assets, processes and value adding services;
- The main threats today and on the horizon; and
- Evidence that business continuity plans are effective.

1.4 Business Continuity and Emergency Management

BC and Emergency Management work together. Emergency Management at the University forms part of the incident management process within the BCM programme. Traditionally, incident management has been associated with the activation of and liaison with the Emergency Services. Emergency management itself is typically seen as the domain of "first responder organisations" such as police, fire, ambulance, government agencies and local authorities (GPG:2013).

Crisis Management is the process by which the University deals with a major incident that threatens to damage the University, interested parties or the general public. This includes incidents that do not necessarily impact the University's ability to deliver services, and includes incidents such as adverse media attention that can damage the University's reputation. In regard to crisis management, the University has established a Critical Incident Management Group (CIMG). This CIMG operates in accordance with the **Critical Incident Policy and Framework (CIP)**.

1.5 Business Continuity Management Lifecycle

This BCM Lifecycle shows the stages of activity the University moves through with the overall aim of improving its resilience.

Figure 1: The BCM lifecycle

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:

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

- Revision of a BIA that identified substantive changes in processes and priorities; or
- A significant change in one or more of the following:
    - The University's risk appetite (i.e. prompted by an incident);
    - Economic/political landscape in relation to the higher education sector;
    - Services and project activities; and
    - Legal or regulatory requirements

The scope is largely determined through available resources, both financial and human resources that is also linked to the risk appetite of the University in the area of business disruption. Adequate resourcing is identified in the BC Policy as being essential for the implementation, ongoing management and validation of the BCM programme.

Divisional Heads and Management across the University support the BC policy by promoting its importance and relevance to their staff. This is accomplished by:

1) Ensuring the BCM programme is compatible with the strategic direction of the University;
2) Ensuring the BCM programme achieves its expected outcomes and requirements;
3) Communicating the importance of effective business continuity management and conforming to the BC policy;
4) Motivating and empowering persons to contribute to the effectiveness of the BCM programme;
5) Providing the resources to establish, implement, operate, monitor, review and improve the BCM programme; and
6) Integrating the BCM programme requirements into the University's business processes

A sustainable BC programme is only possible if the scope is well defined, activities selected are prioritised correctly and people are assigned clear roles and responsibilities within the BC programme. This is communicated throughout the University to build awareness.

2.1 Roles and Responsibilities

Given the scale of the University and scope of activities, a suitable Business Continuity Function Owner (BCFO) is designated from within work areas where essential or urgent business processes or services require business continuity plans. The role of the BCFO is to act as a departmental representative and supports the Chief of Staff Office with:

- Information for the Business Impact Analysis (BIA);
- Developing, implementing and maintaining plans;
- Conducting test exercises;
- Undertaking document revisions;
- Assisting in BC training and awareness activities; and
- Assisting with managing incidents

2.2 Monitoring programme performance

The programme will be managed within the framework and according to the principles contained in the University's BC policy document. The methods that are available to the University to manage its BC programme may include some of the following:

- Self-assessment against a standard, legislation/regulatory requirement(s) or University policy/procedure
- Annual personal performance measurement;
- Supplier and outsource provider relationship management (e.g. JCU Controlled Entities);
- Relationship management of supplier of BC related specialist resources and services;
- Financial management and budget for BCM;
- Independent legal, statutory and regulatory advice
- Industry sector benchmarking; and
- Internal and/or independent audits;

2.3 BC and Supplier Management

This refers to the large number of suppliers of goods and services on which the University depends, but whose providers are unlikely to adopt the same rigour or scrutiny that would be undertaken before a major contract or supply agreement is awarded.

University stakeholders and interested parties expect suppliers to be scrutinised at some level as part of the University due diligence process. The impact of a disruption to a supplier may cause the University both financial and reputational damage. Therefore some knowledge of this exposure is important for the University to understand.

Supply disruption often originates below the immediate, or tier one supplier. This leads to a requirement to ensure key suppliers to the University have also considered their own supply chain continuity within their BCM programme (if they have one). The degree to which the University believes supplier analysis must be undertaken is guided by the risk appetite surrounding the University activity or service potentially impacted by the supplier/service provider.

Critical suppliers or service providers to the University are identified during the BIA stage of the BCM Lifecycle.

Supplier considerations include the following:

- Financial impact of supplier interruption over time;
- Reputational impact of interruption over time; and
- Failure of regulatory compliance caused by interruption

2.4 BC Documentation

BCM Programme documentation has three purposes:

- To enable a prompt and effective response to an incident;
- To help manage the BCM programme effectively; and
- 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:

- All documentation needs to be current. Documents are to be reviewed at 12-monthly intervals to update information, or earlier as changes dictate;
- Documentation needs to be accessible to all business unit staff who may need to use it for carrying out key organisational processes;
- All documentation needs be created and maintained in accordance with the University **Records Management Policy**; and
- 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:

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

- Ensuring the BCM programme is matched to the University's strategic direction and objectives;
- Directing that BC is integrated into business processes;
- Assigning the required resources to develop and maintain the BCM programme;
- Maintaining regular oversight of BCM programme effectiveness; and
- Consultation with everyone involved in developing the BCM programme to help raise awareness;
- Communicating the importance of BC to staff and other interested parties.

3.2 Skills and Competence

Individuals assigned to undertake specific roles within the BCM programme will have the appropriate skills.

General training on BC related issues are provided to staff so they can:

- Recognise an incident;
- Alert JCU Security (or alternate incident response teams depending on incident);
- Contact Emergency Services as appropriate;
- Escalate to the Critical Incident Management Group (CIMG) in accordance with the Incident Management Policy and Critical Incident Procedures;
- Respond appropriately to specific threats;
- Respond appropriately when evacuated from a particular location;
- Understand relevant plans and their role in them; and
- Find out further information about the University's BCM programme

Much of the above training is provided through the Health and Safety Management System and University induction process.

3.3 BC Awareness

The purpose of managing awareness campaigns, is to increase knowledge levels across the University. The benefits mean that BC becomes part of the "fabric" and the 'way we do business". This increases the University's ability to recognise threats, respond in a timely manner and improve the level of resilience.

The awareness campaign will consist of some, or all of the following:

- Distribution of e-bulletins, posters, newsletters, dedicated website and other communications;
- Participation in workshops, seminars, presentations, webinars and test exercises;
- Other BC related promotional activities

BC training includes:

- Online training;
- Presentations at group meetings or to JCU Committees as needed;
- Inclusion of BC subject matter at internal training incidents;
- Discussion of a recent test exercise and learning outcomes; and
- Review of a relevant incident that impacted the University

For each role in the BCM programme, the necessary skills are identified. Individuals are assessed against the skills required and training needs are highlighted and addressed.

4. Business Impact Analysis (BIA)

4.1 What is a Business Impact Analysis?

The BIA looks at the services and activities delivered by the University as well as dependencies that underpin them. For each service/activity within the BCM programme scope, the purpose of a BIA is to:

- document the impacts over time that would result from loss or disruption;
- identify the maximum tolerable period of disruption (or maximum acceptable outage - MAO);
- determine the priorities for recovery; and
- identify the dependencies and resources (both internal and external) required to achieve agreed service levels

ISO 22301 describes the MAO as 'the time within which the impacts of not resuming the activity would become unacceptable.'

The MAO could be reached when the reputation of the University is so badly damaged through a legal or regulatory failure that interested parties no longer want to be associated with it, or external pressure from interested parties forces a major change in the University's strategy.

Service delivery, process or activity failures can result in one or more of the following:

- Health implications from an internal biosecurity failure or external pandemic emergency;
- Breaches of statutory duties or regulatory requirements
- Financial impacts from fewer student enrolments
- Environmental damage
- Set-backs on research projects (e.g. outcomes not delivering or funding no longer provided)
- Opportunities for other higher education providers (domestically and internationally) to increase market share

Seasonality and variability affects the University MAO and is difficult to determine. Examples of University seasonality or peak demand periods include student enrolment periods and examination/assessment times. To account for this, the BIA examines interruptions to an activity during vulnerable periods of peak delivery, regulatory compliance or limited resource as well as steady state operations.

Where a process might involve an unknown lead time, assumptions are made in setting the MAO.

The following diagram illustrates how business continuity can be effective in mitigating impacts in certain situations (in this case a sudden disruption). Some of the diagrammatic terms are matched with labels relating to descriptions of key terms. The RTO and MBCO in *Figure 2* are activity or service specific and can vary.

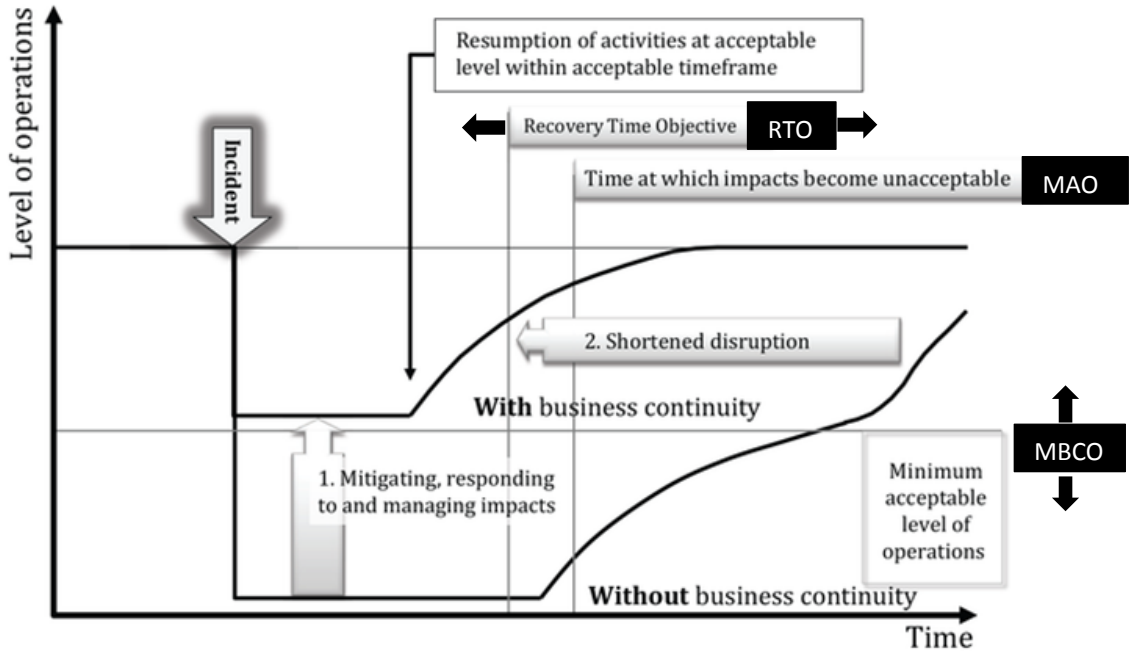


Figure 2: Illustration of business continuity being effective for sudden disruption (excerpt from ISO22313:2012). No particular timescales are implied by the relative distance between the stages depicted in the diagram.

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:

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

- Understanding the potential impact of significant future developments within the University or the environment within which it operates;
- For analysis purposes, assigning the services/activities of the University to business/work units based on urgency of delivery, splitting by key stakeholder/partners and location as relevant;
- Agreeing impacts to be considered as well as the criteria to determine the level of unacceptability;
- Documenting impacts to the University in units of time, of a failure to deliver services/activities;
- Estimating a MAO for each service/activity and seeking agreement with the project sponsor;
- Identifying business processes across the University that deliver the services (may cut across several departments);
- Identifying business continuity function owners for each process and suitable staff, such as subject matter experts, to provide information about the business processes;
- Identifying how and when a disruption to the process could result in damage to the delivery of services;
- Reviewing specific impacts which might not be fully understood such as:
    - Backlogs and capacity issues;
    - The duration or lead time of the process;
    - Any non-standard or unique activities which are difficult to recover and could unexpectedly delay the resumption of the process; and
    - Presenting the findings to Audit, Risk and Compliance Committee of JCU Council for review and approval

4.3 BIA Methods and Tools

Methods and tools used in combination to carry out an initial BIA include:

- Workshops;
- Questionnaire(s); and
- Interviews

A *BIA spreadsheet template* has been created to record individual BIAs across the University. The type of information collected on separate templates comprising the BIA is shown in *Appendix A-F* and includes the following:

1. **Identify priority services and/or activities carried out within BCM scope:**
    a. Name of product or service
    b. Critical Activity (What are the main activities required to deliver the service)
    c. Working patterns
    d. Seasonal Variations (Identify peak/critical time of year/month)
    e. Service Level Agreements (time schedules if they exist)
    f. Departments dependent on
    g. Departments who are dependent on you
    h. ICT applications used
    i. Suppliers Used
    j. Key contact numbers

2. **Impact (consequence) definitions based on the 7 strategic risk areas identified in the University Plan and Risk Management Framework:**
    a. Workplace Health and Safety

b. Financial
c. Compliance and Liability
d. Reputation
e. People
f. Learning and Teaching
g. Research

3. **Service/activity impact:**
   a. Disruption risk rating for each area identified in item 2 above for each activity/service in BCM scope.
   b. MAO and RTO is estimated prior to finalisation in the *Design of Recovery Strategies* detailed in Section 5.

4. **Supplier assessment**
   a. Any supplier with an unacceptable level of impact within 1 week will need to be reviewed to determine their level of resilience.
   b. For new potential suppliers, this will involve doing due diligence to assess their level of business continuity before signing a contract.
   c. For existing suppliers, a review of the Service Level Agreement in place for awareness of operational risk. Amend contract at next review.

5. **ICT applications**
   a. Findings of the ICT Applications impact assessment are used to create a register of key applications that support the delivery of priority services.
   b. Prioritisation applied to disaster recovery planning.

6. **Continuity Resourcing Requirements**
   a. Determine minimum number of resources required over time to continue delivery of services within the RTO.

The BIA identifies both the urgency of service delivery and the activities which enable that delivery. Mitigation measures target the most urgent activities within the University, thus improving the likely return on investment and minimise impact during disruption.

4. Design of Recovery Strategies

5.1 General

The purpose of designing continuity and recovery strategies (and tactics) is to set timescales for recovery and identify the means by which those objectives are achieved. This is undertaken at three levels, determined by the University and based on scale and complexity:

- Strategic – services;
- Tactical – process infrastructure; and
- Operational – activities that deliver the services

An example is shown below to illustrate the importance of recovery strategies and where they fit into University process thinking:

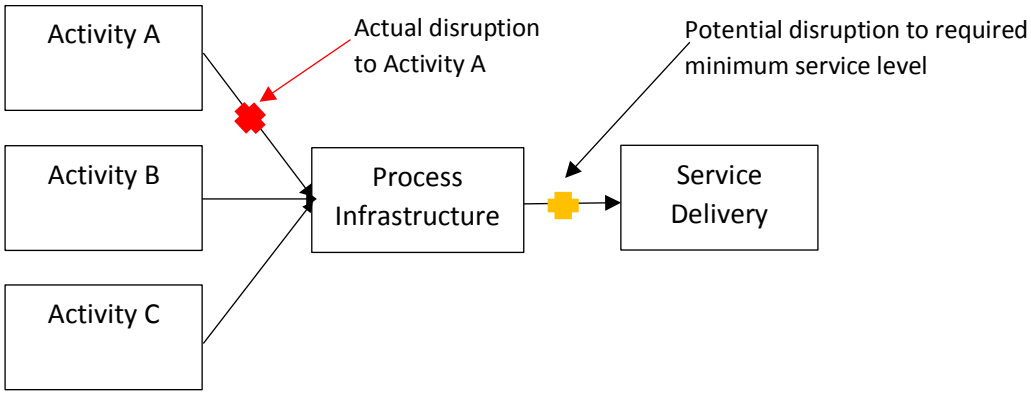


Figure 3a: Recovery strategy for Activity A needed. Minimum required service level not impacted (i.e. MBCO below normal, but not breached).

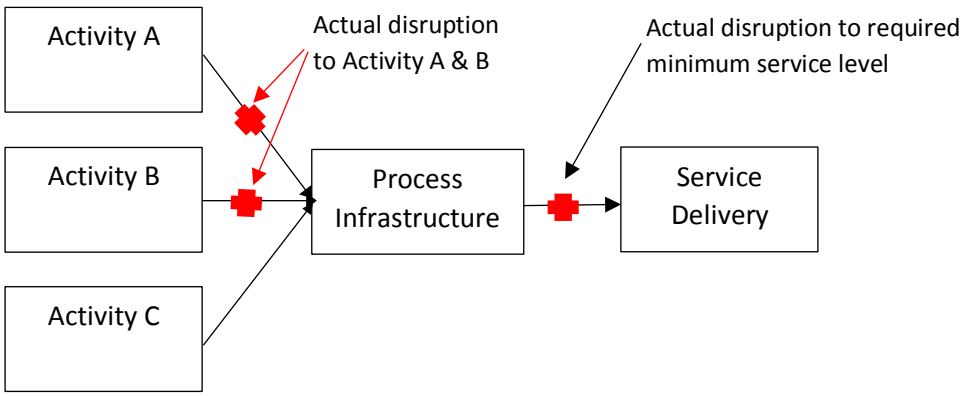


Figure 3b: Activity A and B disruption resulting in disruption of required service to below minimum level (i.e. MBCO has been breached).

An alternative scenario to the above is one where there is no disruption to activities, but process infrastructure has suffered a disruption resulting in failure of the required service.

This Design stage sets the agreed period of time for the resumption of activities, processes and services (RTO) as outlined in the above example.

NOTE: The aggregate RTO of processes, activities and dependent services must not exceed the MAO of the overall process.

A number of general strategies for continuity and recovery have been identified, allocated to a particular service/activity for deployment by the University, as appropriate to a given set of circumstances:

- **Diversification** – using two or more geographically dispersed places. In the event of loss of one process/operation, the activity can continue at the other sites. This strategy is suitable where the *RTO is measured in minutes or hours* rather than days.
- **Replication** - Copying resources to enable operations to be recovered quickly is a variation on diversification in that the replicated site is dormant, being brought into live

operation after an incident. Suitable where the *RTO is greater than a few hours and less than a day or so*.

- **Standby** - Where the *RTO is greater than a day*, a standby facility is available that can be made operational within the RTO. Relies on staff being able and willing to work away from their normal site.
- **Post-incident acquisition** - Acquiring the resources required to undertake activities after an incident from a list of requirements. Suitable for *RTOs measured in days or weeks*. Depends on having pre-qualified suppliers providing resources at short notice. Not appropriate where there is `a requirement for specialist equipment, facilities or skills.
- **Do nothing** - Waiting until after the incident to decide what to do. Appropriate strategy where the *RTO is measured in months*, but only where specialised equipment, facilities or skills are not required that have long lead times, etc.
- **Subcontracting** - Third parties used for services, provide process infrastructure and undertake certain activities.

Insurance is a strategy used to provide financial compensation for loss and disruption and covers expenditure outlays to return to pre interruption levels (e.g. relocation of staff, lost research equipment and loss of income generating activities through consultancies). Continuity strategies selected must consider insurance cover the University has arranged and insurance policy exclusions understood. Insurance will not provide cover for loss of reputation or legislative/regulatory breaches.

5.2 Process for designing recovery strategies

The key steps in the design process, which need to be undertaken for each service/activity within the scope of the BCM programme include:

- Identify the MAO and deciding the RTO (such that the RTO is less than the MAO);
- If a phased level of resumption is required, identify RTOs for each service level;
- If the process infrastructure or activities provide or use data, decide the RPO;
- Where there are existing processes or procedures, conduct a “gap analysis” to identify where existing performance is measured against the required performance;
- Identify suitable strategies that will enable each RTO and RPO to be achieved;
- Analyse the strategic/tactical options for effectiveness and cost; and
- Provide Audit, Risk and Compliance Committee of JCU Council an evaluation of the options, findings and recommendations.
- Identifying implementation projects for each of the options selected and include in Divisional or Business Unit plans.

5.3 Threat mitigation

The purpose of designing threat mitigation measures is to identify and select proactive measures that can be implemented to reduce the likelihood and/or consequence of disruption to the University’s most time critical and urgent activities. The ULRA can be used as a source of threats already identified as part of a risk analysis process.

Where deemed necessary a cost/benefit analysis will be undertaken to determine whether the cost of implementing a measure outweighs the benefit in terms of likelihood and/or consequence of a disruption, should a threat be realised. Examples of threat mitigation measures adopted by the University include:

- Physical security
- Information security
- Monitoring systems to warn of fire and utility failures and other equipment failures
- Sprinkler systems and fire suppression systems

5.4 Incident Response Structure

The purpose of designing an incident response structure is to ensure a documented and fully understood mechanism for responding to an incident that has the potential to cause disruption to the University, regardless of its cause.

An incident response structure identifies:

- The teams responsible for response and recovery activity;
- The relationships between the teams; and
- The roles and responsibilities of the teams

Further information is contained in the JCU Incident Management Policy and Critical Incident Procedures which takes into account the management structure, scale and complexity of the University, its process infrastructure, continuity and recovery strategies and urgency of recovery requirements including communication.

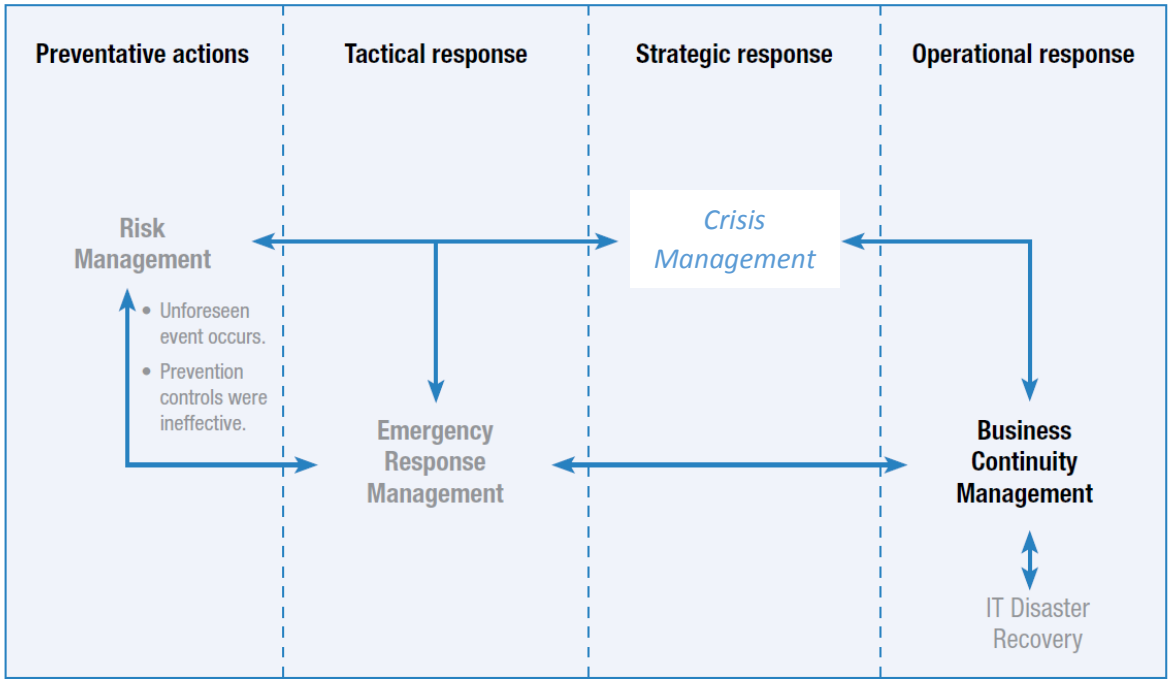


Figure 4: The relationship between risk, emergency response, incident and business continuity management in managing a business disruption.

Source: Adapted from Australian National Audit Office, Business Continuity Management, Building resilience in public sector entities, Better Practice Guide, June 2009

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. The levels of response to be implemented need to reflect the geographical diversity. This in itself provides greater flexibility in designing and adopting any of the recovery strategies identified in Section 5.1.

A University hierarchy of Business Continuity planning and response is proposed below:

Table 1: BCP hierarchy

Level	Application at JCU	Coverage	Response team
Strategic Crisis Management Plan	Incident Management Policy and Critical Incident Procedures	Whole of University (Townsville, Cairns Singapore and Bris.)	Critical Incident Management Group
Tactical Business Continuity Plan	May involve a number of separate BCPs according to campus location and nature of incident/disaster	Individual Division, and/or campus location. Includes JCU Controlled Entities as applicable.	Each Division has a response team consisting of BC functional owners, and people responsible for areas identified in the BCPs
Operational Business Unit and Functional Support Resumption plans	Operational plan for business support functions such as ICT, Finance, HR and JCU sites/facilities	Colleges, business support functions and other JCU sites and facilities.	Each College, support function or site/facility has its own response team (operational staff). May involve some people from Tactical

Because the tactical and operational plans contain information about recovery, they cannot be developed until the BC strategy and tactical options have been determined and agreed.

Each plan contains assumptions about the maximum scale of the incident that it has been designed for and addresses extent, duration or impact.

6.3 Developing a BCP

The key steps in developing a plan include:

- Appoint an owner/sponsor for the plan (e.g. BCFO);
- Define the objectives and scope;
- Develop and approve a plan development process;
- Create a planning team (2-4 people);
- Agree the responsibilities of the response team and their relationship with other plans and response teams (strategic, tactical and operational);
- Create a response team having the required skills;
- Decide the structure, format, components and content of the plan;
- Determine the strategies, such as alternative locations, on which the plan will be based;
- Gather information to populate the plan;
- Draft the plan;
- Circulate the draft plan for consultation, review and feedback;
- Amend the plan as appropriate;
- Agree and validate the plan, for example by rehearsing through test exercises; and
- Agree a programme of ongoing exercising and maintenance of the plan to ensure it remains current and response teams are up to date (refer Section 7.4)

Meetings, interviews, checklists and workshops are used to carry out the activities above.

All plans at all levels contain a number of similar elements:

Table 2: Plan structure and contents

1. Purpose and scope	9. Invocation (of recovery arrangements)
2. Objectives and assumptions	10. Contact details (usually held as appendices)
3. Incident management structure (for the organisation as a whole)	11. Team meeting room (command centre) locations
4. Response team responsibilities	12. Communications (covering employees, contractors, interested parties, customers and the media);
5. Response team membership (leader, primary members and deputies)	13. Key information from previous stages of the BCM lifecycle, such as details of the organization's prioritised activities and timeframes
6. Individual responsibilities of the team members	14. Action lists
7. Team mobilisation (instructions)	15. Procedures for standing down the team and organisation once the disruptive incident has been resolved
8. Plan Activation (procedures and authorisation	

6.4 Tactical Plans

Specific steps in developing tactical plans include the following actions:

- Appoint a person(s) to manage the development of plans within the relevant Divisional area (e.g. BCFO);
- Develop a planning process and schedule. This begins with plans for the highest priority services/activities;

- 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:

- Promptly respond to activation;
- Assess information and make decisions (Go/No Go);
- Mobilise the teams and invoke resources;
- Initiate response procedures and recovery activities;
- Communicate and receive information from other teams; and
- Monitor progress and report status to the CIMG as per escalation process in the CIP.

Available resources include checklists or registers with details of:

- Staff;
- Welfare requirements;
- Alternative locations;
- Security arrangements;
- Technology, communications and data;
- Transportation and logistics;
- Other service providers and suppliers;
- Contact information to access those resources; and
- Resource requirements for resumption of each activity

6.4.1 Review of planning process

Information can become out of date quickly, such as contact details, and are reviewed regularly, in line with the BC policy. Other information is formally reviewed at pre-defined intervals and validated through test exercises (Validation stage of BCM lifecycle).

Other triggers leading to review include:

- A significant organisational change (e.g. restructure);
- A major University process change (policy or procedural);
- A significant change in staffing levels; and
- A significant change in ICT services

6.5 Operational Plans

Operational level plans cover the response by individual departments or business units to the incident.

Examples of operational level plans are:

- A College level or business unit plan to resume its functions within a predefined timescale;
- An HR response to welfare issues during an incident;
- Procedures to assist a tactical level team, often led by a department that deals with the physical incident response and recovery; and
- An ICT department's response to the loss and subsequent resumption of ICT applications and infrastructure services to the University

Operational plans are action orientated and easy to reference under stressful conditions. It must not include information or documents that are not required during an incident.

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:

- Staff welfare;
- Access to and use of facilities;
- Resumption of business unit activities within agreed recovery time objective levels;
- Liaison with IT service continuity teams; and
- 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:

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

- 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
- 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
- Develop and maintain professional relationships and effective two-way communication between the media industry and members of the University community

7. Validation of the BCM Programme

7.1 General

The purpose of Validation is to ensure that BC capability of the University reflects its scale and complexity and that University capability is current, accurate, and complete, and that actions are taken to continually improve resilience.

Validation is achieved through the following three activities:

- Testing;
- Maintenance; and
- Review

7.2 Testing the BCM Programme

A planned Testing Programme is required to ensure that all aspects of the University response to an incident have been tested, in particular:

- All information in plans is verified;
- All plans are rehearsed; and
- All relevant personnel (including deputies) are well practiced

The aims of exercising University BCPs include:

- Evaluating current BC capability;
- Identifying areas for improvement or missing information;
- Highlighting assumptions which need to be questioned;
- Instilling confidence in participants involved in testing exercises;
- Developing team work;
- Raising awareness of BC throughout the University; and
- Testing the effectiveness and timeliness of recovery procedures.

Members of an incident response team as defined in the relevant BCP are to be involved in scenario testing every 12 months.

The University's BC policy, BC programme management (Section 2) and Embedding Business continuity (Section 3.2) address how the testing/exercising regime is to be planned and managed, specialist training undertaken and necessary resources identified.

7.3 Process for testing BCM

- Review the scope (plans, recovery resources and activities) of past tests to identify areas not recently tested;
- Raise with Senior Management any perceived areas of weakness and exercising priorities;
- Determine budget for the BCM testing programme;
- Decide on suitable types of testing for the areas to be assessed for a 12 month plan
- Check the availability of required staff and facilities;
- Develop a test exercise schedule;
- Discuss approval with Senior Management; and
- Identify training requirements for participants and integrate with the test exercise schedule.

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. Participants are expected to be familiar with the plans being exercised and are required to demonstrate how these plans work as the scenario unfolds.
c. Desk top exercises can be a realistic, cost effective and efficient method.
d. Can be greatly enhanced by the use of media (mock) which can make a scenario more realistic.

7.4.3 Simulation

a. Typically involves management teams at a strategic, tactical or operational level
b. Participants can be located across the whole University (and could potentially involve willing interested parties), all working from their usual day to day locations.
c. Participants are given information in a way that simulates a real incident. Participants are expected to deal with the situations they encounter as if it were a real situation.
d. Has the added advantage of testing information flow, communication and equipment, in addition to procedures, decision making and coordination.

7.4.4 Real Time exercise

a. Real time exercises can range from a small scale rehearsal of one component of the response, for example laboratory evacuation, through to a full scale rehearsal involving a section of the University using colour coded JCU Campus Map zoning – Appendix H
b. Real time exercises are designed to include everyone likely to be involved in that part of the response. This type of exercise is particularly useful where there is a legal or regulatory requirement or where a high risk to the University has been identified and the response and recovery plans need to be fully tested.
c. The most appropriate and realistic way to train people and test plans.
d. Resources required can be significant and there may be financial implications
e. Care must be taken to avoid disruption to the normal operation and any reputational impact must be considered

7.5 Developing a test exercise or scenario

Careful planning is required. The chance of disruption caused by the exercise and the impact of any potential disruption must be minimised and the residual risk of something going wrong must be understood and accepted by Management.

People involved in exercises can include some of the following depending on the scenario:

- Facilitator;
- Observer(s);
- Strategic, Tactical, Operational level incident response teams as appropriate;
- BC Function Owners/representatives from various Divisions;
- Suppliers of recovery resources and services;
- Emergency services;
- Local authority emergency planners;
- Subject matter experts; and
- Internal auditor(s)

The process adopted by the University for developing a test exercise is:

- Agree the scope, aims, objectives and expected outcomes of the exercise;
- Identify the exercise planning team (3-6 people);
- Design – plan and design the exercise, including setting a budget and conducting a risk assessment to identify the risks of an impact on University operations, where appropriate;
- Conduct – run the exercise;
- De-brief – assess and report the outcome, including a de-brief of the participants immediately after the exercise; and
- Follow-up – address any issues arising from the test exercise by:.
    - Recording the test exercise and findings in the Riskware Audit/Inspection Register; and
    - Enter, assign responsibility and monitor completion of improvement actions

7.5.1 Outcomes of the test exercise

A number of benefits can be gained from the test exercise programme and include:

- Validation that the BC Programme is effective. To confirm this, key risk indicators (KRIs) have been developed to monitor performance. KRIs include:
    - Number of test exercises undertaken as planned (planned vs. actual)
    - Number improvement actions generated from test exercises
    - Number of lessons learned from exercises not addressed by certain timeframe
    - % members of response teams involved in a testing exercise each year
    - Estimation and improvement of RTO and MAO accuracy (+/- 5%, +/-10%, etc.)
- Confirmation that team members and staff are familiar with their roles, responsibilities and authority in response to an incident;
- Validation of the technical, logistical, administration aspects of the BCP(s);
- Confirmation of the recovery infrastructure (command centres, work areas, technology and telecommunications, etc.);
- Confirmation of the availability of staff and processes for relocation;
- Documentation of exercise results in a post exercise report for Top Management, auditors, insurers, legal bodies and regulators as appropriate;
- Documentation and resolution of issues identified during the exercise;
- An increased awareness of emergency procedures;
- An increased awareness of the significance of BC;

7.6 Maintenance

Maintenance of the BCM programme keeps the University's BC arrangements up to date, ensuring preparedness to respond and manage incidents effectively, despite constant change.

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:

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

To improve effectiveness, BC maintenance activities are embedded within the University's management processes including Divisional triennium planning and general budget planning cycles. Aspects of BCM performance monitoring are included the Operational Performance Targets (OPTs) for each Division.

7.6.1 Process

A formal process for maintaining the BCM programme has been established. The process is undertaken at planned intervals, the frequency of which depend on the nature of the change. For instance, contact details will potentially require updating on a six monthly basis, compared to revising the BC policy on a two yearly basis.

Responsibility for undertaking the planned maintenance process is given to an individual or team, within a business unit or work area with responsibility for BC. The maintenance process consists of:

- Reviewing what has changed since the last update;
- Analysing the impact of any changes by:
    - Reviewing and challenging any assumptions that have been made;
    - Determining whether any time objectives have changed;
    - Determining the adequacy and availability of external services that might be required such as asset refurbishment, recovery sites and subcontracts; and
    - Reviewing the Business Continuity arrangements of key suppliers;

- Update BC plans as required;
- Identify any flow-on effects to other areas;
- Advise those responsible in other areas of the flow-on effects;
- Assess whether amendments create a training need, awareness campaign and/or communication need;
- Provide training, awareness and/or communications as required;
- If BC plans have been changed, distribute the new versions as appropriate (QA process);
- Identify the date for undertaking the next planned maintenance, and schedule the maintenance.

Maintenance activities form part of the University suite of key risk indicators relating to the area of Business Disruption (JCU risk consequence criteria). The KRIs extend beyond specific indicators used to monitor ICT performance. KRIs, relating to maintenance activities are monitored and reported against periodically and include;

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:

- **Audit (internal and external)** – a formal independent review process that incorporates elements of the University's BCM programme and measures its effectiveness against a pre-agreed standard to assess resilience;

- **Self-Assessment** – an assessment of the BCM programme as it relates to a Division or business unit by the area responsible for BC. Uses a centrally distributed and agreed *self-assessment template - Appendix G*.

- **Quality Assurance (QA)** – a process that ensures various outputs from the BCM programme meet overall University requirements (as deemed necessary or triggered by an incident resulting from a policy or procedural deficiency);

- **Performance Appraisal** – a review of the performance of individuals (against relevant KPIs such as number of plans completed or expenditure against budget) in relation to their BC roles and responsibilities; and

- **Supplier Performance** – Supplier performance is reviewed against contractual Service Level Agreements (SLAs). This is related to key suppliers identified in the BIA stage. Conclusions can be made in relation to a supplier BCM programme.

The University's Annual Internal Audit Work Plan, when targeting the University BCM programme, aims to:

- Validate compliance with the University's BC policy and implementation of the BC Management Plan against relevant standards (e.g. ISO 22301:2012 or AS/NZS 5050:2010), legislation or regulations; or
- Review the University's BCM programme (BCM lifecycle performance); or
- Validate the University BCP or Divisional BCPs; or
- Verify that appropriate test exercises and maintenance activities have occurred; and
- Highlight deficiencies and issues and ensure their resolution

It is important that maintenance and review of the BCM programme is ongoing. This will help to ensure resilience is enhanced in support of achieving the University's strategic objectives.

An assurance program is established covering the 5 types of review and is shown below:

Table 3: BCM Programme Assurance

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

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

8. Definitions

Term	Definition
Business Continuity	The capability of the University to continue delivery of services at acceptable predefined levels following a disruptive event (e.g. cyclone, cyber- attack, etc.). Definition from ISO 22300
Business Continuity Policy (BC Policy)	The key document that sets out scope and governance of the BCM programme. The policy reflects the reasons for why the programme is being implemented (GPG2013)
Business Continuity Management Programme (BCM programme)	Ongoing management and governance process supported by the University Executive and Council of JCU. The BC programme is appropriately resourced to implement and maintain business continuity management (ISO 22301)
Business Continuity Management System (BCMS)	Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity (ISO 22301)
Business Continuity Plan (BCP)	Documented procedures that guide the University to respond, recover, resume and restore to a predefined level of operation following disruption (ISO 22301)
Business Impact Analysis (BIA)	Process of analysing University activities and the impact that a business interruption might have on those activities (ISO 22301)
Business Continuity Lifecycle (BCM Lifecycle)	A series of business continuity activities which collectively cover all phases of the BCM programme (GPG2013)
Critical Incident Management Group	The Critical Incident Management Group is the body of people convened by the Chief Coordinator to manage the University's response to a Critical Incident
Chief Coordinator	Chief of Staff, or Vice-Chancellor's nominee
Disruption	Breakdown or failure of an activity, process or service resulting in a loss (financial, human physical, etc.) and occurs over an uncertain period of time. See "incident"

Incident	Situation that might be, or could lead to, a disruption, loss, emergency or crisis (ISO 22300:2012)
Invocation	Act of declaring that the University's business continuity arrangements need to be put into effect in order to continue delivery of key products and services (adapted from ISO 22301:2012)
Maximum Acceptable Outage (MAO)	The time taken for adverse impacts that might arise as a result of not providing a service or performing an activity, to become unacceptable (ISO 22301:2012). The duration after which the University's viability will be threatened if a service or function cannot be resumed.
Minimum Business Continuity Objective (MBCO)	A minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption (ISO 22301:2012)
Recovery Time Objective	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)
Recovery Point Objective	The point to which information used by an activity must be restored to enable the activity to operate on resumption. Also referred to as Maximum Data Loss (ISO 22301:2012)
Resilience	The capability to anticipate key events from emerging trends, constantly adapt to change and to bounce back from disruptive and damaging incidents (GPG2013). The University's ability to achieve its immediate objectives in uncertain and non-routine times.
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation (ISO 31000)
Risk Management	Coordinated activities to direct and control an organization with regard to risk (ISO 31000)
Stakeholder/Interested party	Those people and organisations who may affect, be affected by, or perceive themselves to be affected by, a decision or activity (ISO 22301:2012)
Threat	Potential cause of an unwanted incident, which can result in harm to individuals, a system or organisation (ISO 22300:2012)
Test/Exercise	A process to train for, assess, practice and improve performance in an organisation (ISO 22301:2012)
Test Programme	Series of exercise events designed to meet an overall objective (ISO 22300:2012)

Appendix A – Services Register

Department: _____ *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*	Working patterns	***Seasonal Variations*** *Identify peak/critical time of year/month*	Service Level Agreements *Time schedules*	Departments you are dependent on	Departments who are dependent on you	IT applications used	Suppliers Used	Key Telephone numbers e.g. Customer contact point
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

Once you have completed the Business Impact Analysis, please update the 'Date last reviewed' & 'Completed by', then email to the Business Continuity Manager: *[insert email address and ext. number]*

Appendix B – Impact Definitions

BUSINESS IMPACT DEFINITIONS							
Impact		**Financial**		**Compliance & Liability**		**Learning and Teaching**	
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 fatlaity 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 between 1 month and 1 semester; Loss of mandatory accreditation of single course; localised fraud or misconduct in academic activities including enrolments and examination processes
Catastrophic	Multiple fatality, prosecution or legislative non-compliance impacts a substantial part or whole of University with significant works > $500k.	Catastrophic	one off loss of > $50m	Catastrophic	Successful class actions or serious prosecution, repeated breaches of significant contractual arrangements, significant statutory intervention due to serious breach of legislation	Catastrophic	inability to deliver face to face courses > 1 semester; Loss of accreditation of multiple courses; institutionalised and/or systemic fraud or misconduct in academic activities including enrolments and examination processes
Reputation		**People**		**Research**			
Insignificant	One off media enquiries or neutral press coverage	Insignificant	one off localised negative impact on morale	Insignificant	loss of research project (< $y)		
Minor	One off negative local publicity not requiring management intervention	Minor	Inability to attract or retain key staff in specialised area; negative impact on morale in a Division	Minor	loss of research project (>$y and < $x)		
Moderate	One off negative publicity requiring some management resources to deal with	Moderate	inability to attract or retain key staff in one or two disciplines; negative impact on morale across university	Moderate	loss of significant research project		
Major	Significant negative publicity resulting in some loss of funding, staff and/or students	Major	One off failure to properly deal with serious grievances; inability to attract or retain key staff in multiple disciplines; significant staff unrest and/or industrial action at Division level	Major	loss of multiple significant research projects		
Catastrophic	Sustained negative national and international publicity resulting in significant loss of funding, staff and/or students	Catastrophic	Systemic failure to properly deal with serious grievances; sustained high levels of staff turnover across entire university; university-wide staff unrest and/or sustained industrial action	Catastrophic	loss of flagship research projects		

Appendix C – Service/Activity Impact Assessment

Name of Product or Service 0

Maximum Acceptable Outage		Recovery Time Objective

WHS

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

REPUTATION

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

PEOPLE

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

FINANCE

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

LEGAL

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

LEARNING & TEACHING

IMPACT	4 hrs	1 day	2 DAYS	1 week	1 month	
No Impact						
Minor						
Moderate						
Major			x			
Critical						

RESEARCH

IMPACT	4 HRS	1 day	2 days	1 week	1 month	
No Impact						
Minor						
Moderate						
Major	x					
Critical						

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:*

- *WHS*
- *Reputation*
- *People*
- *Finance*
- *Legal*
- *Learning and Teaching*
- *Research*

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

[Name of supplier]		Time					Justification
		4 hrs	1 day	2 days	1 week	1 month	
IMPACT	No Impact						
	Minor						
	Moderate						
	Major						
	Critical						

[Name of supplier]		Time					Justification
		4 hrs	1 day	2 days	1 week	1 month	
IMPACT	No Impact						
	Minor						
	Moderate						
	Major						
	Critical						

[Name of supplier]		Time					Justification
		4 hrs	1 day	2 days	1 week	1 month	
IMPACT	No Impact						
	Minor						
	Moderate						
	Major						
	Critical						

[Name of supplier]		Time					Justification
		4 hrs	1 day	2 days	1 week	1 month	
IMPACT	No Impact						
	Minor						
	Moderate						
	Major						
	Critical						

[Name of supplier]		Time					Justification
		4 hrs	1 day	2 days	1 week	1 month	
IMPACT	No Impact						
	Minor						
	Moderate						
	Major						
	Critical						

Any supplier with an unacceptable level of impact within 1 week will need to be reviewed to determine their level of resilience.

For new potential suppliers, this will involve doing due diligience to assess their level of business continuity before signing a contract. If the supplier has appropriate business continuity arrangements, then you will need to include a business continuity schedule in the Service Level Agreement that reflects the findings of your due diligence. Your company may also decide to dual contract the resource to reduce risk.

For existing suppliers, you may want to review the Service Level Agreement in place so you are aware of operational risk and can amend the contract in the next review (where appropriate).

Appendix E – ICT Applications Assessment

[Name of IT application]		Purpose What is the application used for?					
		Workaround exists Yes / No					
		With any existing workarounds in place, what is the impact over time if this application was unavailable					Justification
		4 hrs	1 day	2 days	1 week	1 month	
IMPACT	No Impact						
	Minor						
	Moderate						
	Major						
	Critical						

[Name of IT application]		Purpose What is the application used for?					
		Workaround exists Yes / No					
		With any existing workarounds in place, what is the impact over time if this application was unavailable					Justification
		4 hrs	1 day	2 days	1 week	1 month	
IMPACT	No Impact						
	Minor						
	Moderate						
	Major						
	Critical						

[Name of IT application]		Purpose What is the application used for?					
		Workaround exists Yes / No					
		With any existing workarounds in place, what is the impact over time if this application was unavailable					Justification
		4 hrs	1 day	2 days	1 week	1 month	
IMPACT	No Impact						
	Minor						
	Moderate						
	Major						
	Critical						

[Name of IT application]		Purpose What is the application used for?					
		Workaround exists Yes / No					
		With any existing workarounds in place, what is the impact over time if this application was unavailable					Justification
		4 hrs	1 day	2 days	1 week	1 month	
IMPACT	No Impact						
	Minor						
	Moderate						
	Major						
	Critical						

The findings of the IT Applications impact assessment will be used to create a register of key applications that support the delivery of business key products and services. The register will be used to prioritise disaster recovery planning.

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*	*Specialist Equip.*
4 hours										X	
1 day										X	
2 days										X	
1 week										X	
1 month										X	

Examples of other resources you may wish to include: work mobile, printer, scanner, hardcopy documents, specialist equipment.

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
Responsibility and Ownership				
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 responsibilities for BC and delivery of critical activities/services			
RO3	Managers and employees have been briefed in the last twelve months and understand 1) what will be involved in an incident recovery; 2) what level of recovery to services/activities is needed; and 3) what is expected of staff			
Governance and Reporting				
GR1	Appropriate reporting procedures are in place to monitor business continuity capability at business or support function level			
GR2	Governance and reporting processes as they relate to BCM outputs are documented and detail how deficiencies are communicated and escalated			
GR3	Business continuity is a standing agenda item at operational review meetings or similar where BC issues are raised and actions decided			
Planning Process and BCP Scope				
P1	All planning is based on threats identified in the: a) documented risk assessment (ULRA, Divisional, Project or Activity); b) Division/Business unit and ICT planning Business Impact Analysis (BIA)			
P2	Recovery priorities for business-critical processes/services and vital records are identified; Recovery Time Objective (RTO) and Recovery Point Objective (RPO) established and documented. MAO is defined			
P3	Alternate sites used for work areas are located at least 5km away (where off-campus) from the primary site, or alternate campus location - zone colour (Appendix H). Facilities have maintained Uninterrupted Power Supply (UPS), standby generators and diverse routing for communications (data and voice). Confirm with ICT.			

Ref. No.	Area of Assessment / Questions	Score		Comments
Review				
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: a) following test exercises where deficiencies are identified b) following incidents including near-misses c) following changes to BIA			
Testing and Incidents				
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			
T3	All testing is documented - covering aims, methodology, results, remedial actions as required, timescales and ownership, learning points and next steps. Findings entered in Riskware database for monitoring and reporting			
Outsourced services and Key Suppliers				
OS1	Outsourced functions meet the University's management and operational / policy requirements			
OS2	Monitoring and reporting procedures are in place to monitor the business continuity capability of outsourced functions/critical suppliers			
OS3	Critical suppliers or outsourced services have formal agreements or arrangements in place that specify a notification and escalation process, including current supplier/outsource provider contact details			
	Results of Self-Assessment		**90**	
	Performance <45 = Red; 45-67 = Amber; 68-90 = Green			**Based on the actual or adjusted score (refer Note below)**
	Recommendations (provided to Risk Champion by Risk and Compliance Officer):			

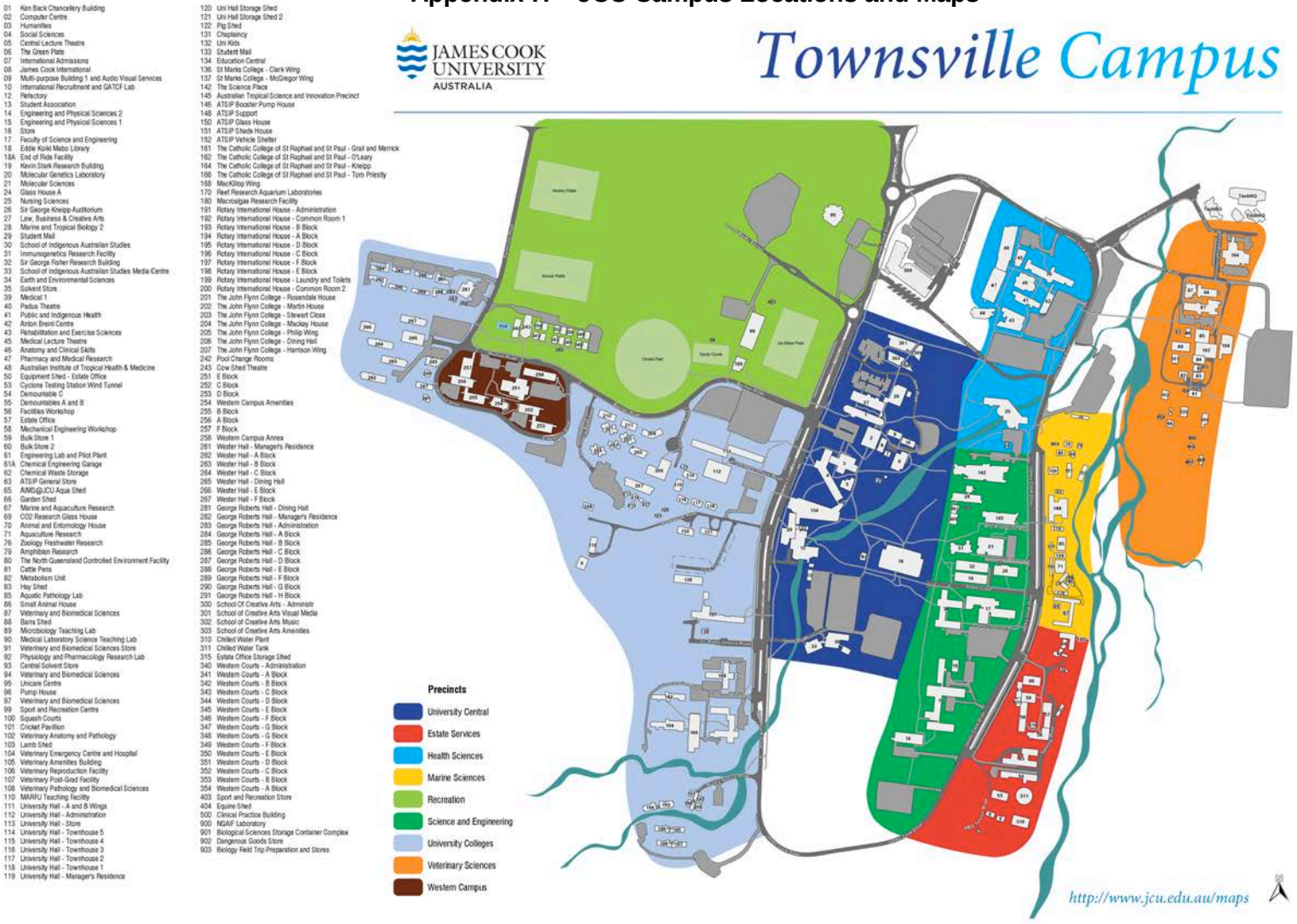
Self-Assessment Scoring: 'Yes' = 3 (100%); Mostly = 2 (>75%); Partial = 1 (50-75%); 'No' = 0 (<50%)

Completed Self-Assessments must be returned to the Risk and Compliance Officer aaron.ginzburg@jcu.edu.au

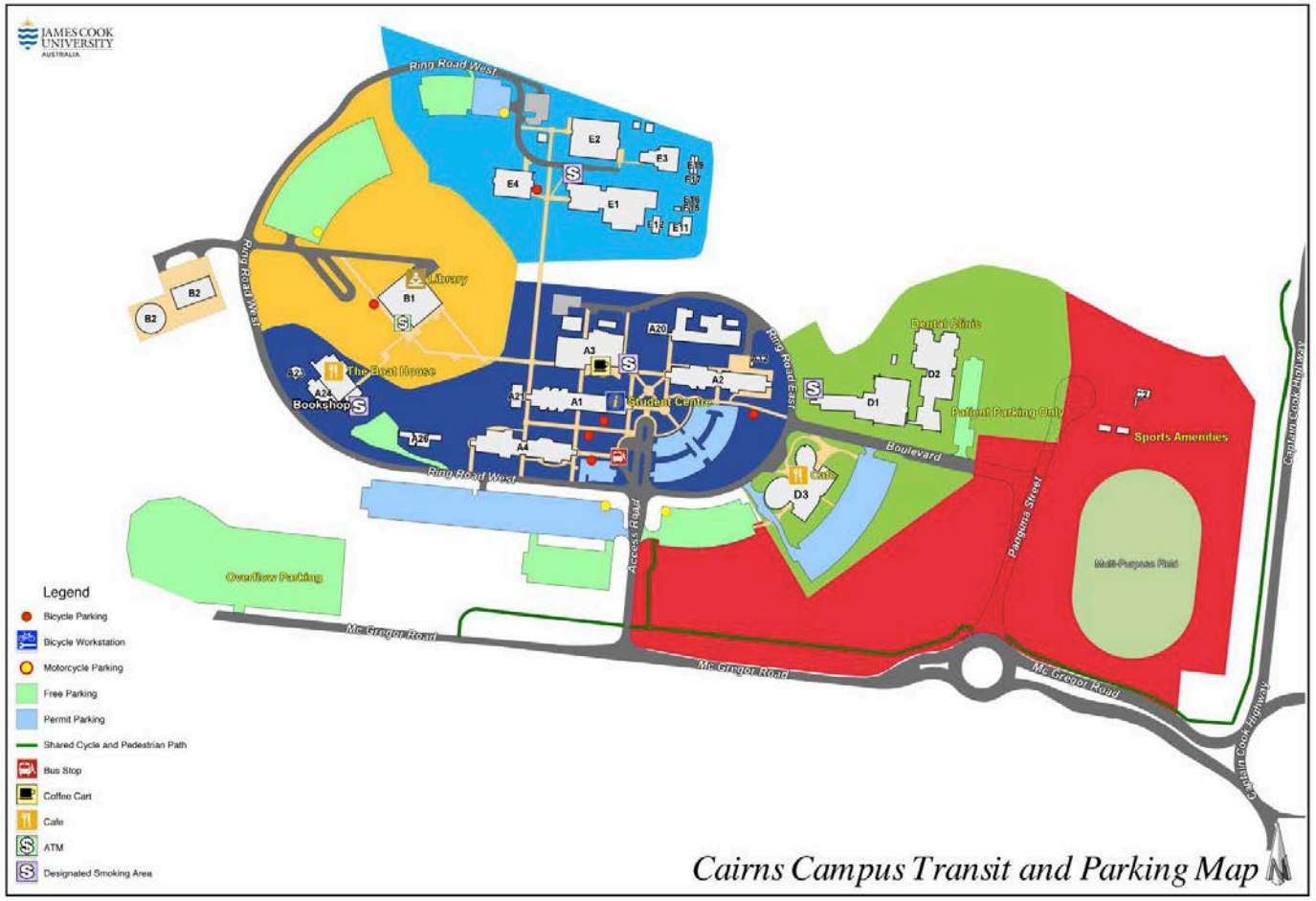
Note: Where **Y** or **M** is selected, evidence must be referenced in comments section (as a minimum), or provided as an attachment. If no evidence is available, the score will be reassigned to **N,** impacting on the overall performance outcome.

JAMES COOK UNIVERSITY AUSTRALIA

Appendix H – JCU Campus Locations and Maps

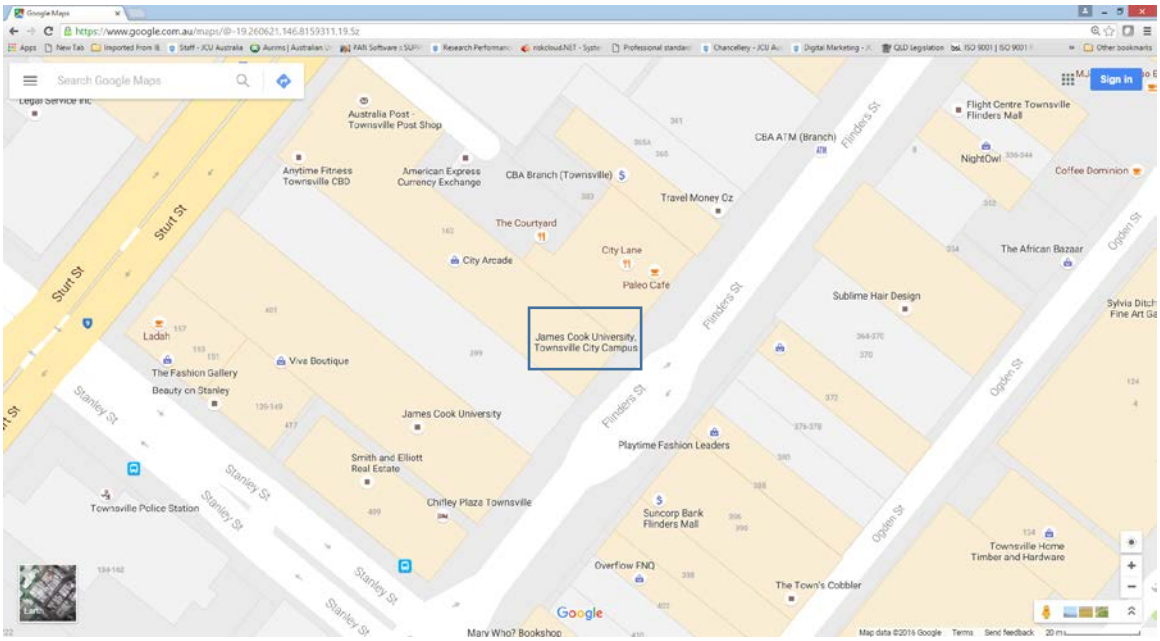


JAMES COOK UNIVERSITY AUSTRALIA



JCU Townsville City campus and street map

383 Flinders St



JCU Cairns City campus and street map

36 Shields St