Business Continuity Management Framework

(Includes Emergency, Critical and Local Incident Management)
7.2. Testing ............................................................................................................................. 30
7.3. Review and Maintenance ............................................................................................... 31
8. APPENDICES:..................................................................................................................... 32
  8.1. Definitions .................................................................................................................... 32
  8.2. Business Continuity Planning Guide - Planning Considerations ................................ 34
  8.3. Document Information ............................................................................................... 37
1. Introduction

1.1 Purpose of this Framework

The Business Continuity Management Framework exists to protect UWA’s people, animals, reputation and assets and aid strategic achievement. Starting with management of the incident itself (Emergency, Critical or Local Incidents), the business continuity management system should if priority processes, equipment and infrastructure are impacted and then provide the Business Unit (BU) with the information and guidance to restore them (e.g. via Critical Incident Response Plans (CIRPs) and Business Continuity Plans (BCPs)).

This Framework is designed to assist management and staff of UWA to comply with the UWA BCM Policy and implement and manage the elements of BCM. It is also to be used to familiarise new managers and staff with the relevant processes.

UWA’s BCM framework applies to all University controlled operations/functions, regardless of the location in which they are undertaken. The framework does not include the operations/functions of the University’s external stakeholders/vendors etc.

This framework does not contain information on specific requirements and strategies for recovery. These are detailed in the Critical Incident Response Plan and specific business units’ BCPs.

1.2. Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCM</td>
<td>Business Continuity Management</td>
<td>A holistic process managing the University’s activities to ensure effective management of a material disruption, and the maintenance and restoration of priority processes with minimal impact to staff, students and the general community</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Plan</td>
<td>A set of documents with instructions and procedures to enable Business Units to respond to accidents, disasters, emergencies and threats to ensure minimal disruption to priority processes</td>
</tr>
<tr>
<td>BIA</td>
<td>Business Impact Analysis</td>
<td>A detailed risk analysis that examines the nature and extent of disruptions and the likelihood of the resulting consequences and collects data to assist in restoration of priority processes/functions for use in the BCP.</td>
</tr>
<tr>
<td>BRC</td>
<td>Business Recovery Coordinator</td>
<td>To liaise with and coordinate recovery activities with the BU, and BRT members</td>
</tr>
<tr>
<td>BRT</td>
<td>Business Recovery Team</td>
<td>Specific members of a business that perform required actions to manage the business recovery activities</td>
</tr>
<tr>
<td>BU</td>
<td>Business Unit</td>
<td>A part of a company that operates as a separate part of the whole business. For instance, Campus Operations as a part of Campus Management, or a School as part of a faculty.</td>
</tr>
<tr>
<td>CIM</td>
<td>Critical Incident Management</td>
<td>The initial management of a disruption impacting one or more UWA Business Units which could lead to reputational damage or the failure or institutional level operations</td>
</tr>
<tr>
<td>CIMT</td>
<td>Critical Incident Management Team</td>
<td>The team responsible for the initial management of a disruption impacting one or more UWA Business Units which could lead to reputational damage or the failure to meet UWA’s objectives</td>
</tr>
<tr>
<td>CIRP</td>
<td>Critical Incident Response Plan</td>
<td>A set of documents with instructions and procedures to enable CIMT to respond to in an institutional level to assessed critical incidents.</td>
</tr>
<tr>
<td>DR</td>
<td>Disaster Recovery</td>
<td>Activities relate to the actions to resume IT Services and are managed by IT Services or a business unit’s own IT staff</td>
</tr>
<tr>
<td>MAO</td>
<td>Maximum Allowable Outage</td>
<td>Maximum period of time that the University can tolerate the disruption of a critical business process.</td>
</tr>
</tbody>
</table>
2. What is Business Continuity Management?

The objective of the BCM program is to ensure the continuity of the University’s priority processes, equipment and infrastructure. The Business Continuity Management Policy states the following as UWA’s business continuity aim:

“to achieve the University’s resilience and response capability in order to safeguard people and operations and ensure we can continue to achieve its education, research and community engagement goals.”

BCM is a continuous improvement process of establishing and maintaining Critical Incident Response Plans (CIRP), Business Continuity Plans (BCP) and other measures in order to respond to and recover from disruptions. Collectively these measures are referred to as the University’s BCM capability.

This diagram represents the relationship between the components of the University’s BCM capability:

### 2.1. Emergency Incident Management

An emergency is a situation that poses an immediate risk to health, life, property or the environment. Most emergencies require urgent intervention to prevent a worsening of the situation before it adversely affects the occupants or visitors to UWA.

Some emergencies (e.g. fire requiring building evacuation) have documented Emergency Management Plans to enable management and staff to quickly and decisively respond to an emergency, which could threaten the safety of persons or property on-campus, or disrupt campus operations.

These events will usually controlled by UWA Security with the assistance of the Emergency Control Organisation (ECO) of the impacted building. External services such as the Fire Department, Ambulance and Police may also be involved, in which case they will assume control and liaise directly with UWA Security.

An emergency may also have the potential to escalate to a critical incident due to the effect on UWA’s reputation, priority operations and functions. If this occurs, it will escalate to a critical incident and be managed by the Critical Incident Management Team (CIMT).

**Note:** Not all emergencies become critical incidents e.g. a broken leg may require Emergency Services (Ambulance) but not an institutional response.

All emergencies will be communicated to UWA Security (ext 2222) so that they can decide whether or not to declare the event a critical incident. If there is doubt, then the event is treated as reportable i.e. take the most conservative approach.

These events include but are not limited to:

- Fire
- Injury requiring emergency services response
- Death of one or more person(s)
- Personal threat
- Bomb threat
- Suspicious mail or package
- Gas, chemical, biological and radioisotope spill or leak
2.1.1. Emergency Control Organisation (ECO) Structure

The Emergency Control Organisation is a structured organisation of people employed within a building who take command on the declaration of an emergency, pending the arrival of the fire brigade or other emergency service.

It is comprised of UWA staff including Security, Health Safety & Wellbeing, Specialists (chemical experts, lab staff etc.) and then, in each building, Building Wardens, Deputy Building Wardens, Area Wardens and First Aid Personnel.

Please refer to the Safety Health & Wellbeing website – “Responsibility and Duty of the Emergency Control Organisation” for full information.

2.2. Critical Incident Management

Critical Incident Management is the initial management of a material disruption that requires an institutional response due to possible impacts on UWA’s objectives and/or reputation. Such incidents are managed by the Critical Incident Management Team (CIMT) and commonly last 1-14 days.

Response priorities will be determined in the following order:

1. People
2. Animals
3. Reputation
4. Assets

In practice these priorities will usually be addressed simultaneously to protect all aspects of university business. Material disruptions that could result in a critical incident being declared include:

- Large scale fire/explosion
- Fatal accident
- High value fraud
- Natural disaster
- Strike action by staff or students
- Epidemic or pandemic
- Extended IT outage e.g. due to cyber attack
- Forecasted major storm (e.g. cyclone) or major event (e.g. volatile protest, planned major utility outage) where preparatory actions are required to be undertaken to protect people, animals, reputation and/or assets.
2.2.1. CIMT Structure

The CIMT is led by a CIMT Chair and CIMT Leadership Team comprised of the Communications Controller, Planning/Intelligence Controller, Operations Controller & Logistics Controller.

They in turn have assigned roles reporting them. The membership of the CIMT is determined by the CIMT Chair and can change during the management of the incident.

The following depicts the structure of the Critical Incident Management Team:

**2.2.2. Delegations**

Via the BCM policy, the Vice Chancellor has given the CIMT a delegated responsibility to exceed normal financial and decision making delegations where insufficient time exists to obtain normal approvals, due to the urgency or risk related to the incident. This extraordinary right extends for as long as the CIMT is actively managing a critical incident.

This right is effective from the time of critical incident declaration to closure of the incident. Upon hand-over, normal delegations resume for both CIMT members and the business unit.

**Note:** The misuse of the delegation rights noted above may be considered misconduct and any suspected cases of abuse will be reported to the Senior Deputy Vice Chancellor.
2.3. Local Incident Management

This is the management of an incident by local Business Unit management.

The incident may impact one or more Business Units but the overall impact is not considered to be a threat to UWA’s reputation, priority processes, equipment and infrastructure and/or is not likely to result in sustained media attention i.e. not a Critical incident.

Local incident management may require the activation of the Business Continuity Plan (BCP). For example, a small fire destroys a single piece of equipment in use by the Business Unit but does not require a Fire Department response. Local incident management involves putting out the fire, ensuring the safety of staff, students and others, notifications to management and stakeholders and arranging for clean-up and replacement of lost items. It may also require relocating an activity that utilised the equipment until it is replaced. However it ends when those actions are completed.

It may require activation of a BCP that is in place for specific types of events. These plans assist the Business Unit to manage the incident itself.

Local incidents include but are not limited to:
- Loss of IT systems where they are owned and maintained by the Business Unit (external to BITS)
- Small scale fire/flood where process impacts are relatively minor and media attention is not likely
- Loss of power to a building and therefore failure of a temperature controlled environment.

2.3.1. Local Incident Management Team Structure

Local Incident Management Team structures can vary. It can consist of the Business Unit internal senior management team or they may assign a Business Recovery Coordinator and define team members to support them. Regardless of the membership, they will manage the incident and may or may not activate their BCP to do so.

2.4. Business Recovery

This is the process of restoring the priority processes, equipment and infrastructure of a Business Unit. Where priority processes, equipment and infrastructure exist, this is managed via a Business Continuity Plan (BCP). The BCP is required only where priority 1 processes, equipment and infrastructure (refer Section 5) have been identified, otherwise it falls under business as usual processes to restore operations.

A BCP may be activated after the urgent aspects of an incident are dealt with or it may run concurrently with the management of the incident. The activation of a BCP could continue for a number of months depending on how long restoration activities take.

2.5. Technology Recovery

Information Technology (IT) Disaster Recovery (DR) activities relate to the actions undertaken to resume IT services after a disruption and are managed by Business Information & Technology Services (BITS) for institutional systems, or a Business Unit’s local IT staff for locally managed systems. It can be managed as a local incident or more generally as part of a formal IT DR Plan.

2.6. Full Restoration

These are the activities required to restore and return all affected operations to their original state, not just the restart of priority 1 processes, equipment or infrastructure i.e. restoration of priority 2&3 processes). This may include the reversal of actions taken to recover priority 1 processes e.g. to enable a return to the primary site, or the move to a new permanent location.
3. Business Continuity Management Framework Responsibilities

Within the University’s BCM program, the following University stakeholders play an important role with specific responsibilities:

**The Senate** has the ultimate responsibility for oversight of Risk Management and BCM across the University.

**The Audit & Risk Committee** is responsible, by delegation from the Senate, for ensuring that the University embeds and maintains adequate BCM processes, culture and reporting mechanisms.

**The Vice-Chancellor (VC)** has the overall executive accountability for the University’s business continuity capability and overall executive responsibility for the University’s critical incident response.

**The Senior Deputy Vice Chancellor (SDVC)** has direct executive responsibility for the overall BCM framework delivery sponsorship and support.

**Deans, Directors, Heads of Schools, Faculty and School and Centre Managers** are responsible for ensuring that BCM is integrated into their business as an operational discipline that is appropriately resourced, supported and that a suitable culture is promoted.

**UWA Security** has the responsibility to monitor and assist with the personal safety of staff, students and visitors whilst on campus and to provide services to protect personal security such as night transport, security officers and barriers. They are also responsible for:
- providing a first aid response service to the campus
- co-ordinating the emergency response to fires, bomb threats, explosions, gas leaks, storms and other dangerous incidents

**The Emergency Control Organisation (ECO)** is established to ensure all buildings have been provided with personnel with the required resources and training to enable prompt incident response. They are also responsible for:
- The safety of the occupants and visitors in their building during an emergency. As a principle, the ECO will focus firstly on the safety of staff, students and visitors before considering UWA assets and other matters.
- Each member of the ECO will be responsible for their documented duties as per the Emergency Management Plan.

**The Associate Director Risk & Legal and the Strategic Risk Manager** are responsible for:
- Coordinating the BCM Framework and supporting the University in achieving an acceptable continuity capability, culture and sourcing and adopting the methodology and tools to enable BCM implementation.
- Ensuring that the BCM Framework reflects relevant strategic and operational risks.
- Facilitating and assisting in the development and review of BCM strategies (including critical incident management and BCPs) to ensure conformance with the policy.
- Reporting to the Executive and Audit & Risk Committee on BCM policy and framework compliance.
- Ensuring the CIMT is comprised of suitably skilled and experienced staff, including the identification of appropriate alternates for key CIMT roles.
- Maintenance of the Critical Incident Response Plan (CIRP) and associated training processes.
- Act as one of the “Authorised Persons” to give approval for security and medical evacuation of staff & students by a third party provider.
The Business Continuity Manager is responsible for:

- Developing a framework, methodology and tools to enable BCM implementation across the University.
- Providing the central co-ordination, operational support, reporting and monitoring of all University BCM initiatives.
- Facilitating and assisting in the development and review of BCM strategies (including critical incident management, BCPs and a BCM culture) to ensure conformance with the policy.
- Assisting the CIMT to manage critical incidents as required. In particular, acting as the link between local Business Units and the CIMT when local BCPs and critical incidents are activated at the same time, or in sequence.
- Maintenance of the CIRP and training process.
- Ensuring appropriate reference to strategic and operational risks when developing BCPs.
- Monitoring and reporting compliance with the policy and framework to the Strategic Risk Manager, and facilitating training and awareness initiatives.
- Liaising with key centralised UWA Operational Business Units (e.g. Campus Management, BITS) to share relevant continuity information.
- Review and gap analysis post critical incident (or near miss) & BCP activation.

4. CIMT Notification, Activation and Stand Down Processes

Incidents can and do occur at any time of the day and night. It is the nature and severity that determines the level of incident response.

The following table shows examples of how different incident types might be dealt with:

<table>
<thead>
<tr>
<th>Incident Management Type</th>
<th>Incident</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Incident (without BCP activation)</td>
<td>A fire contained within a fume hood and put out using a fire extinguisher.</td>
<td>Damage to fume hood requiring replacement. Resulting in inability to continue operations that utilise the fume hood. BCP not activated as there was no impact to priority process, equipment or infrastructure.</td>
</tr>
<tr>
<td>Emergency Incident</td>
<td>A fire started in a fume hood and extends into the room. Fire alarms triggered and Fire Wardens evacuate building. Fire Department responds.</td>
<td>Damage including short term power loss to 2 floors. All operations on these floors have ceased. BCP activated to restore operations</td>
</tr>
<tr>
<td>Local Incident (with BCP activation)</td>
<td>A fire started in a fume hood engulfs and destroys the building. Fire alarms triggered and Fire Wardens evacuate building. Fire Department responds.</td>
<td>Damage renders building inhabitable for the foreseeable future. All operations in the building cease. CIMT activated to manage institutional response BCP activated to restore key Business Unit operations</td>
</tr>
<tr>
<td>Emergency Incident</td>
<td>Severe storm/Cyclone forecasted in next 3-5 days. Possible severe impacts to UWA location</td>
<td>Due to the threat to people, animals and property, CIMT can be activated to ensure preparatory actions are being taken. For instance: preparation of sand bags, evacuation in remote location etc.</td>
</tr>
</tbody>
</table>

Note: Refer Section 4.1 Incident Risk Assessment Matrix to assess incident level
### 4.1. Incident Assessment

The following Incident Risk Assessment Matrix has been developed to assist with rating UWA incidents.

A Major or Extreme rating requires the CIMT Chair to **activate** the CIMT. A Moderate rating requires the CIMT Chair to be **notified**; however the CIMT Chair will then determine if CIMT activation is required.

If CIMT is activated, the CIMT Chair will mobilise the required CIMT members and manage the institutional level responses and will engage with the business unit(s) and external emergency services as required.

**Note:** Where the impact of an incident may not be clear, engagement of the CIMT Chair is required to make the decision.

The following provides guidance on assessing the rating of the incident and when the CIMT might be activated:

<table>
<thead>
<tr>
<th>Risk</th>
<th>Incident Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Extreme</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Notifications:</strong></td>
<td></td>
</tr>
<tr>
<td>1. Security</td>
<td></td>
</tr>
<tr>
<td>2. Critical Incident Management Team</td>
<td></td>
</tr>
<tr>
<td>3. Business Management</td>
<td></td>
</tr>
</tbody>
</table>

- **Injury/Health Threat:** Death or Permanent Disability requiring institutional level response or where there are known broad impact(s) on campus or public stakeholders
- **General Services:** Interruption to services of more than 72hrs
- **Loss of Power or Critical IT Services:** Interruption to services of more than 24hrs
- **Environmental:** Irreversible environmental harm or permanent negative impact.
- **Financial:** Loss>$10m:
  - Direct Loss
  - Loss of Opportunity
  - Lost Revenue
  - Increased cost
- **Reputation:** Exposure to widespread national news profile. Formal Inquiry State or Federal Level. Cyber-attack with known loss of critical intellectual property or key data sets. E.g. Loss of student or staff personal data.
- **Legal Ramifications:** Major Breach of statutory obligation or major contractual default with significant penalties and or severe judgments against the organization
- **Forecasted:** Where a planned or forecasted event (major storm/cyclone, violent or widespread protest, utility shutdown) has a high level of probability to result in any of the above impacts.
<table>
<thead>
<tr>
<th>Risk</th>
<th>Incident Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Major</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **Notifications:** | 1. Security  
2. Critical Incident Management Team  
3. Business Management |
| **Injury/Health Threat:** | Life threatening injury or multiple serious injuries requiring institutional level response or where there is the potential for high impact on campus or public stakeholders |
| **General Services:** | Interruption to services of 24-72hrs |
| **Loss of Power or Critical IT Services:** | Interruption to services of 8-24hrs |
| **Environmental:** | Major environmental impact; requires long term recovery or has a long term negative impact |
| **Financial:** | Loss $1m to $10m  
- Direct Loss  
- Loss of opportunity  
- Lost Revenue  
- Increased cost |
| **Reputation:** | High news profile, third party action, government involvement, cyber-attack with loss of intellectual property or key data sets. |
| **Legal Ramifications:** | Major breach of statutory obligations resulting in fine or civil litigation by individual or group either private or corporate |
| **Forecasted:** | Where a planned or forecasted event (large scale storm, protest, utility shutdown) could reasonably result in any of the above impacts |

<table>
<thead>
<tr>
<th>Risk</th>
<th>Incident Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Moderate</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **Notifications:** | 1. Security  
2. Critical Incident Management Team  
3. Business Management |
| **Injury/Health Threat:** | Serious injury requiring medical treatment or where there is the potential to impact on campus or public stakeholders |
| **General Services:** | Interruption to services of 8-24hrs |
| **Loss of Power or Critical IT Services:** | Interruption to services of 0-8hrs |
| **Environmental:** | Environmental impact of a small nature requiring a long term recovery |
| **Financial:** | Loss of >$250k to $1m.  
- Direct Loss  
- Loss of opportunity  
- Lost Revenue  
- Increased cost |
<p>| <strong>Reputation:</strong> | Public embarrassment moderate news coverage (local and state media). Cyber-attack with potential loss of intellectual property or key data sets. |
| <strong>Legal Ramifications:</strong> | Significant breach of statutory or contractual obligations. Resulting in a fine or contractual penalty |
| <strong>Forecasted:</strong> | Where a planned or forecasted event could reasonably result in any of the above impacts and CIMT to be notified for proactive discussion. |</p>
<table>
<thead>
<tr>
<th>Risk</th>
<th>Incident Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minor</td>
<td><strong>Injury:</strong> Minor injury or first aid treatment.</td>
</tr>
<tr>
<td></td>
<td><strong>General Services:</strong> Interruption to services of up to 8hrs.</td>
</tr>
<tr>
<td></td>
<td><strong>Loss of Power or Critical IT Services:</strong> Move immediately to Moderate or above</td>
</tr>
<tr>
<td></td>
<td><strong>Environmental:</strong> Small environmental impact – no long term effect or short term</td>
</tr>
<tr>
<td></td>
<td>negative impact</td>
</tr>
<tr>
<td></td>
<td><strong>Financial:</strong> Loss of $50k to $1m:</td>
</tr>
<tr>
<td></td>
<td>• Direct Loss</td>
</tr>
<tr>
<td></td>
<td>• Loss of opportunity</td>
</tr>
<tr>
<td></td>
<td>• Lost Revenue</td>
</tr>
<tr>
<td></td>
<td>• Increased cost, or</td>
</tr>
<tr>
<td></td>
<td><strong>Reputation:</strong> Minor media interest with a low news profile e.g. local paper</td>
</tr>
<tr>
<td></td>
<td><strong>Legal Ramifications:</strong> Minor breach of statutory or contractual obligations</td>
</tr>
</tbody>
</table>
4.2. Incident Notification & Activation Process Map (All Incident Types)

The following process map outlines the notification process and the response outcomes from activation. If the notifications do not occur, the required activations of ECO, CIRP or BCP may not occur.
4.3. Emergency Incident Notification, Activation and Stand Down

UWA Security play a key role in Emergency Incident Management. The management of incidents includes, but is not limited to, the response actions, communication to all parties and directing emergency services to the incident site.

While automatic fire alarm detection and notification or “break glass” units are in place in most large buildings, contact with UWA Security (ext 2222 or +61 6488 2222) is essential.

There may be locations or situations where dialling ‘000’ is required (e.g. locations off the main campus and urgent medical or personal threat situations). These should also be followed by contact with UWA Security as soon as possible afterwards.

Local members of the Emergency Control Organisation (ECO) (e.g. Fire Wardens) may also need to be advised and in some circumstances senior management, CIMT leadership and other stakeholders.

Where the impact of an incident may not be clear, engagement of the CIMT Chair is required to decide if an incident is considered a critical incident. Security will notify the CIMT when required. The notification of the CIMT Chair can be done directly or using the OCA software SMS and Email alert functionality.

UWA Security and the ECO will manage the incident and engage the Business Unit as required. Upon completion of the immediate response (including critical incident response if needed), the remaining restoration activities will be handed back to the business unit. This may or may not require activation of the Business Unit BCP under a local incident management process.

Upon completion of the incident management requirements, the ECO will stand down.

4.4. Local Incident Notification, Activation and Stand Down

4.4.1. Notification

Notification of a local incident is to be made to senior management of the Business Unit. Notification may also be required to other key stakeholders.

If any priority process, equipment and/or infrastructure are impacted, the senior management of the Business Unit is to engage the local Business Recovery Coordinator (BRC) to review the incident’s impacts and determine if activation of the BCP is required.

The following depicts the notification process for contacting the local Business Unit management team (Business Recovery Team) to manage the requirements of the BCP:
4.4.2. Activation of BCP

If the BCP requires activation the UWA Business Continuity Manager (or Strategic Risk Manager) is to be contacted. They will then agree activation of the BCP is required, taking into consideration if any CIMT actions are underway, and whether any other Business Units are impacted. The local Business Recovery Team (BRT) will then undertake the response actions.

4.4.3. Stand Down of (local) Business Recovery Team

Upon completion of the incident management requirements, the local BRT will stand down. Where the BCP was activated, a gap analysis will be required to identify learnings and implement any amendments to the BCP. This will be undertaken by the Risk & Legal Division. The Business Unit should contact the UWA Business Continuity Manager to facilitate this.

4.5. Critical Incident Management Team Notification, Activation and Stand Down

4.5.1. Notification of the incident to the CIMT

Notification to the CIMT Chair must occur:
- When it is identified that there institutional level responses are required
- When it is identified that there institutional level responses may be required in the near future due to an imminent event (e.g. Major storm/cyclone warning issued, bush fire reported nearby, major utility works planned etc.)
- if the incident reporter is unsure if institutional level responses required

Notification is to be made to UWA Security in all cases. UWA Security will immediately log an incident into the Organise, Communicate, Act (OCA) system, which initiates the formal CIMT Notification Process. OCA will issue SMS and Email alerts to the CIMT Leadership Team. The CIMT Chair is then required to acknowledge the alert and assess the incident to determine if CIMT activation is required.

4.5.1.1. Automated CIMT Notification Process - Organise, Communicate, Act (OCA) System

The OCA system is a software application utilised by UWA Security and CIMT to issue notifications to the CIMT Chair of a possible critical incident. It also allows the CIMT Chair to mobilise the required members of the CIMT and to record actions, decisions and outcomes during the incident.

When an incident is created in the OCA System, there is an option to activate CIMT. This will trigger SMS and Email alerts to be issued to the CIMT Leadership Team, made up of the CIMT Chair, CIMT Chair Alternates and the Communications, Planning/intelligence, Logistics and Operations Controllers and their Alternates. The CIMT Chair is then to accept the notification (via SMS or Email response) and determine if it is to be treated as a critical incident.

There are 4 alerts issued to the CIMT Leadership Team with the first addressed to the CIMT Chair requesting they assume the CIMT Chair role and acknowledge the OCA alert. If unable to acknowledge the alert, a second will be issued to the CIMT Leadership Team requesting the CIMT Chair Alternates to accept the role and acknowledge the OCA alert.

Should no CIMT Chair Alternate accept the role and acknowledge the OCA alert, a third alert is issued to the CIMT Leadership Team addressed to the Controllers requesting one to acknowledge the alert and assume the CIMT Chair role. UWA Security will receive the final alert informing them of the inability of any of the CIMT Leadership Team to accept the CIMT Chair role if none of the CIMT Leadership Team respond to the SMS or Email alert.
The following depicts the OCA CIMT Notification Process and alert scripts:

4.5.1.2. Manual CIMT Chair Notification process

If the OCA System is not operational, direct contact to the CIMT is required. The incident reporter is to contact UWA Security who will then contact the CIMT Chair.

However if the CIMT Chair is not available, UWA Security is to contact the CIMT Alternates and members of the CIMT Leadership team and Executive until the CIMT Chair role is assumed. The order of contact is outlined below and determined due to knowledge or UWA and experience in incident management. Subject to change:

<table>
<thead>
<tr>
<th>CIMT Chair, CIMT Chair Alternates &amp; Leadership Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. CIMT Chair</td>
</tr>
<tr>
<td>2. CIMT Chair Alternate 1</td>
</tr>
<tr>
<td>3. CIMT Chair Alternate 2</td>
</tr>
<tr>
<td>4. Logistics Controller or Alternate</td>
</tr>
<tr>
<td>5. Planning/Intelligence Controller or Alternate</td>
</tr>
<tr>
<td>6. Operations Controller or Alternate</td>
</tr>
<tr>
<td>7. Communications Controller or Alternate</td>
</tr>
<tr>
<td>8. Strategic Risk Manager</td>
</tr>
<tr>
<td>9. Senior Deputy Vic Chancellor</td>
</tr>
<tr>
<td>10. Other member of UWA Executive</td>
</tr>
</tbody>
</table>
4.5.2. Activation of CIMT

The CIMT Chair will in all cases assess the incident to determine if the CIMT is to be activated to respond to the incident reported.

If the incident is not to be regarded as a Critical Incident, the “CIMT Required Flag” in OCA is to be returned to “NO” and commentary applied to the Combined Events Log and the decision communicated to the incident reporter.

4.5.3. CIMT Mobilisation

When the CIMT Chair has declared a Critical Incident, they will mobilise the required team members to assist in managing the incident. The membership of the CIMT for managing any incident can comprise the full CIMT or a subset, depending on the scale of the incident. This will be decided by the CIMT Chair. They can be contacted directly or utilising the OCA system.

The University Executive will also be alerted to the incident at this time. An OCA alert can be issued automatically via OCA, or they can be contacted directly by the CIMT Chair or delegate.

The following depicts how OCA Mobilisation alerts operate:

4.5.4. CIMT Rooms

There are 3 rooms available to the CIMT for managing critical incidents. The CIMT are able to request occupants vacate the desired room at any time. The rooms in order of priority (due to completeness of fit out) are:

1. CM Boardroom – 55 Broadway, level 2
2. KJM Multi-Purpose Room - RM-658.216-IS – Ken & Julie Michaels building, level 2

Note: There is no elevator at 55 Broadway, so consider any CIMT members mobility impairment.

4.5.5. CIMT Call Centre

If the need for a dedicated Call-Centre arises, there are two locations immediately available to the CIMT. These are both managed by BI&TS and are:

1. UWA Switchboard – Reid Library – Ground Floor
2. IT Service Desk – K&J Michaels building – 2nd Floor
4.5.6. CIMT Stand down

Upon completion of the immediate response actions, the remaining restoration activities will be handed back to the Business Unit to complete and the CIMT stood down. This may or may not require activation of the Business Unit BCP under a local incident management process. If the BCP is activated, the UWA Business Continuity Manager is also to be engaged.

The CIMT Chair will determine when the CIMT will be stood down.

A gap analysis will be required after stand down of the CIMT. This will be undertaken by Risk & Legal Division.

5. Preparation

5.1. Business Continuity Planning (BCP)

The Business Continuity arrangements of a Business Unit are documented in a BCP. The BCP informs the reader of the priority processes, equipment and infrastructure requiring consideration should an incident occur and provides a guide for recovery, relocation and restoration.

For Business Units, the extent of the planning requirements differs depending on the needs of the Business Unit processes, equipment and/or infrastructure.

A Business Continuity Plan will consist of an action plan to relocate, restore &/or recover the priority items:

- Relocate a process or activity to an alternate location that has been predetermined so that the business needs are already or can be quickly accommodated.
- Restore necessary utilities or other requirements to the priority equipment/machinery in a timely manner to reduce harm to the asset if it cannot be relocated.
- Recover high value artefacts, equipment etc. from the impacted site, undertake restoration actions and relocate to safe location.

The BCP should provide the reader with enough information to ensure the priorities of the Business Unit are restored.

To understand the risks a Business Unit faces during a business disruption, a Business Impact Analysis (BIA) is completed to identify all Business Unit activities requiring specific consideration should an incident arise.

The processes, equipment and/or infrastructure are then assessed using the Maximum Allowable Outage Assessment Matrix (below) and where they are found to be Priority 1, Business Continuity Planning is required. The BIA will then identify all their requirements for those items to input into the BCP.

Understanding these priorities will also assist the Critical Incident Management Team to coordinate their incident management activities.

5.1.1. Step 1 – Undertaking a Business Impact Analysis (BIA)

To understand the risks a Business Unit faces during a business disruption, a Business Impact Analysis (BIA) is completed to assess all Business Unit processes and to identify those requiring specific attention should an incident arise. The Business Unit risk register must also be reviewed to ensure all priorities are identified.

The BIA is a detailed risk analysis that examines the nature and extent of disruptions and the likely consequences on a business process, equipment or infrastructure. A BIA considers the business unit's functions, people, processes, activities, equipment, infrastructure, resources, information, interdependencies and the nature and extent of business disruption over time.

The processes, equipment and/or infrastructure are assessed using the Maximum Allowable Outage (MAO) Assessment Matrix (below) and where they are found to be Priority 1, Business Continuity Planning is required as per the UWA BCM Policy.

Determining MAOs is a key step in the determination of business recovery priority. For a process, equipment and/or infrastructure to require a BCP it must be considered vital to achieving UWA's mission/goals or the business unit's own objectives and require recovery within 5 days. However, if a business wishes to extend the BCP to priority 2 or 3 items it may do so.
MAO estimates are also vital to assist the Business Unit or CIMT to identify the latest timeframe acceptable for the process, equipment and infrastructure to begin to be restored/recovered and operational. This includes ensuring all the resources that are required to undertake the processes are operational and the University service outcome is deliverable.

The following outlines the priority ratings based on maximum allowable outage timeframes:

<table>
<thead>
<tr>
<th>Max Allowable Outage Time</th>
<th>0-4 Hours</th>
<th>4-24 Hours</th>
<th>1-2 Days</th>
<th>2-3 Days</th>
<th>3-7 Days</th>
<th>1-2 Weeks</th>
<th>2-4 Weeks</th>
<th>1-2 Months</th>
<th>&gt; 2 Months</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.1.2. Step 2 – Documenting Business Continuity Plans (BCP)

A BCP is only required where priority processes, equipment and infrastructure are identified. This is due to the Maximum Allowable Outage timelines being less than five days and the business needing to implement actions immediately.

This does not mean that restoration actions are not required for the lower priority processes, equipment or infrastructure, but given the MAO timelines, it is considered that there would be time to recover them after the immediate activity of managing the incident itself and reestablishing Priority 1 items.

The BCP is there to act as a guide to remind a Business Unit of the requirements and important steps needed to resume priority processes. It is not intended to provide full procedural information on undertaking the underlying activities themselves, but needs to ensure adequate detail to assist the reader to complete them correctly.

The BCP will include but is not limited to:

- Critical contact numbers of key Business Unit staff, Critical Incident Management Team and other core UWA Business Units, vendors and other dependents etc. This will enable the notification and escalations to occur as required, and to assist the Business Unit in obtaining the assistance they need in restoring priority processes, equipment and infrastructure promptly.
- An immediate response action plan in bullet point form to ensure actions that must be taken are not forgotten. It includes escalations, notifications and general steps to be actioned as an initial response. It will also refer the reader to the relevant detailed response plan if required.
- A process and/or a scenario based response strategy summary to enable response requirements for priority items.
- Action plans are designed for specific scenarios. For instance:
  - A relocation plan for a priority process,
  - An artefact recovery plan to enter, recover, clean and relocate high value artefacts or artworks
  - A plan to provide portable power to a temperature controlled environment when power is lost to the floor.
  - A plan to relocate teaching or exam activities if venue/s are not available.

Note: This information includes personal contact details. It is therefore to be considered sensitive and appropriate secure storage is required for both hard and soft copies. Misuse of personal contact information may be considered misconduct.

For guidance on what to consider when documenting a BCP refer to Appendix 8.2 – Business Continuity Planning Guide or contact the UWA Business Continuity Manager.
5.2. Specific Business Continuity Planning Roles & Responsibilities

During management of an incident that requires activation of a Business Continuity Plan (BCP), the following stakeholders play an important role with specific responsibilities:

The Vice-Chancellor has the overall executive accountability for the University’s business continuity capability.

The Senior Deputy Vice Chancellor has direct executive responsibility for the overall BCM framework delivery, sponsorship and support.

Deans, Directors, Heads of Schools, Faculty and School and Centre Managers are responsible for ensuring up to date BCPs are created, held and maintained for priority processes, equipment & infrastructure and that a Business Recovery Coordinator is selected and understands their responsibilities.

The Business Recovery Coordinator (BRC) is responsible for:
- Activating the Business Units BCP when required
- Ensuring required actions are undertaken to restore all Business Unit processes with a priority based approach.
- Ensuring the Business Response Team are aware of their responsibilities and the BCP.
- Ensuring the BCP remains up to date.

The Business Recovery Team (BRT) is responsible for ensuring the required actions set out in the BCP are undertaken to resume all Business Unit processes as quickly as possible. This role is usually held by the business management team.

The Strategic Risk Manager is responsible for ensuring there is suitable coverage of the priority processes, equipment and infrastructure and that the BCPs comply with the BCM Framework and Policy. They also ensure that the BCM Framework and associated BCPs reflect relevant strategic and operational risks for the Business Unit and UWA.

The Business Continuity Manager is responsible for assisting Business Units to implement and maintain BCPs where required and to assist the impacted Business Units to manage their business continuity response and complete a post incident review as required. They are also to manage and facilitate training and awareness initiatives.

6. Response

6.1. Critical Incident Response Planning (CIRP)

The Critical Incident Response Plan (CIRP) has been developed to give Executive comfort that critical incidents will be managed effectively. The document also provides direction and guidance to the Critical Incident Management Team Chair (CIMT Chair) and the CIMT in the management of critical incidents.

The CIRP also assist the CIMT to prepare for pending occurrences (e.g. Major storm/cyclone, critical utility works etc.) and ensure prompt response should a critical incident of that nature occur.

The CIRP informs the reader of the critical contacts and also sets out the immediate response actions for the first 60 minutes. It also provides tools and checklists for the CIMT Leadership Teams to ensure vital items are not missed.

The plan includes as a minimum:
- Outline for the processes for notification and mobilization of CIMT (including instructions for use of OCA for these)
- 1st 60 minutes response actions
- Extensive critical contact list including support and advice contacts
- CIMT Leadership Team Checklists
- Scenario Response Checklists (Natural Disaster, Large Protest, Pandemic, Death/Serious Injury, Loss of Power, Loss of Chillers, Site/asset damage)

The CIRP takes a team approach to CIM, with each team member given specific roles and responsibilities before, during and after any critical incident. These roles are linked to their key management competencies.
6.2. Specific Critical Incident Management Team Roles & Responsibilities

During management of a critical incident, the following stakeholders play an important role with specific responsibilities:

The Vice-Chancellor (VC) has the overall executive responsibility for the University's critical incident response. They will also assume the role of the UWA Spokesperson as required.

UWA Spokesperson
The role of the UWA Spokesperson is to act as the public face of the University on matters pertaining to the incident. The Spokesperson takes advice from the CIMT, specifically from the CIMT Chair and the Communications Controller.

The responsibilities of this role are:
- To strategically coordinate and manage all communications (internal and external)
- Protect the University's reputation
- To make public statements
- To ensure the messages are consistent with UWA values
- Ensure that there is consistency in the messages being delivered
- To communicate with the Chancellor and the Senate any matters requiring their attention

The UWA Executive Group is responsible for ensuring they stay abreast of the impacts of the incident to ensure that they are taken into account in making their portfolio decisions. They may also assume the role of the UWA Spokesperson as required if the VC is not available.

Critical Incident Management Team Chair (CIMT Chair)
The role of the CIMT Chair is to determine the incidents that require CIMT management and ensure the CIMT is made up of suitably qualified and experienced members. It is the CIMT Chair's role to ensure the incident is managed in a manner that upholds the University's reputation and values, ensures the safety and wellbeing of all parties involved and the appropriateness of communications made to all stakeholders. The CIMT Chair is the key liaison with the UWA Executive on incident matters.

The responsibilities of this role are:
- To ensure adequate training has been received that is suitable for the role.
- The CIMT roles are held by the appropriate persons (including alternates)
- The members of CIMT understand their roles and responsibilities.
- Appropriate training is undertaken by all members of CIMT and key stakeholders on a regular basis and within 3 months of commencing in the role.
- Appropriate awareness sessions are offered to all staff on a regular basis
- CIMT is activated when required and ensuring appropriate membership for the relevant incident.
- Effective management of the incident and leadership of CIMT.
- Appropriate notifications and communications occur to the UWA Executive (and Senate if required).
- Notification to the VC of decisions made outside of standard delegations (in accordance with BCM Policy)
- The actions taken are carried out in a safe and legally sound manner.
- The agreed actions for the incident are managed to completion in a timely manner.
- Formal closure of the incident.
- The follow-up activities (gap analysis etc.) are undertaken promptly upon closure of a CI event.
- The testing program is undertaken in a timely manner (eg. Desktop testing in accordance with the BCM Framework).
Communications Controller (Comms) and Team

Communications Controller (Comms Controller)
The role of the Comms Controller is to manage the internal & external communication streams, and provide strategic advice to the Chair and the Executive.

The responsibilities of this role are:
- To ensure adequate training has been received that is suitable for the role.
- To determine and tailor the communications strategy and protocols for communications to and from internal and external stakeholders.
- Ensure the prompt notifications and escalations occur to the UWA Executive Team and other required stakeholders.
- The development of communications to all stakeholders and the issuance of communications in a timely manner.
- To ensure staff, students, visitors and the wider public are kept informed regarding impacts to their health and safety.
- To ensure timely escalation to CIMT Chair of any concerns, and to keep the CIMT informed of developments.
- To ensure there is a suitable person on call in all roles within the team at all times and that the contact list for the team is up to date to support CIMT incident notification processes.
- All toolbox items remain up to date.
- Develop and maintain professional relationships with other agencies and departments (i.e. Police, DFES etc).

Media Coordinator
The role of the Media Coordinator is to provide information to and liaise with the media during the incident to ensure timely, accurate and appropriate information is communicated externally and ensure monitoring of external media in relation to the incident.

The responsibilities of this role are:
- To ensure adequate training has been received that is suitable for the role.
- To develop and issue media statements during the incident and ensure the UWA and social media sites are updated as appropriate.
- To take media enquiries and provide responses.
- To contact the University's media monitoring company to ensure close monitoring of media coverage.
- To liaise with external stakeholder media teams as required to ensure consistent and accurate information.
- To monitor external stakeholder websites and news sites to ensure consistent and accurate information.
- To assist the UWA Spokesperson by developing material and providing advice to prepare them for media interviews.
- In consultation with the external agencies and CIMT, determine if media conference/s are required.
- To manage and monitor media on site at the University.
- To provide updates to the CIMT on any items of interest.

Note: The CIMT recognises that communication to the media requires a fast response and pre-approval by the by the CIMT Chair (or P&I Controller by delegation) may not always be possible and is at the discretion of the Media Coordinator.
Internal Communications Coordinator
The role of Internal Comms Coordinator is to use and monitor internal communications at the time of an incident. They will prepare communications for internal and other stakeholders and release them via a suitable medium (including social media).

The responsibilities of this role are:
- To ensure adequate training has been received that is suitable for the role.
- Develop Internal Communications strategy
- To manage the CIMT Call Centre when required
- Identify internal & external stakeholders and act as the liaison for all non-media related communications
- Monitor internal communications and report items of interest to CIMT (excl. social media)
- Prepare internal & stakeholder communications as required and issue when approved by CIMT Chair. (Incl. social media)
- Coordinates responses with the Media, Digital and Student Comms Coordinators
- OCA contact lists maintenance

Note: The CIMT recognises that communications to internal and external stakeholders (excluding media) often requires a prompt response and therefore pre-approval by the CIMT Chair (or Comms Controller by delegation) may not always be possible and release of the communications is at the discretion of the SC Coordinator.

Digital Comms Coordinator
The role of Digital Comms Coordinator is to use and monitor digital platform communications at the time of an incident. They will prepare communications for internal and other stakeholders and release them via a suitable platform.

The responsibilities of this role are:
- To ensure adequate training has been received that is suitable for the role.
- Develop digital communications strategy
- To manage the UWA website when required
- Identify stakeholders and act as the liaison for all digital related communications
- Monitor digital communications and report items of interest to CIMT (Incl social media, web posts etc.)
- Prepare digital communications as required and issue when approved by CIMT Chair. (Incl. staff and student platforms)
- Coordinates responses with the Media, Internal and Student Comms Coordinators
- OCA contact lists maintenance

Note: The CIMT recognises that communications to internal and external stakeholders (excluding media) often requires a prompt response and therefore pre-approval by the CIMT Chair (or Comms Controller by delegation) may not always be possible and release of the communications is at the discretion of the DSM Coordinator.
**Student Comms Coordinator**

The role of Student Comms Coordinator is to use and monitor student communications at the time of an incident. They will prepare communications for internal and other stakeholders and release them via a suitable medium (including social media).

The responsibilities of this role are:

- To ensure adequate training has been received that is suitable for the role.
- Develop student communications strategy
- Identify student stakeholders and act as the liaison for all non-media related communications
- Monitor student communications and report items of interest to CIMT (excl. social media)
- Prepare student communications as required and issue when approved by CIMT Chair. (Incl. social media)
- Coordinates responses with the Media, Internal and Digital Comms Coordinators
- OCA contact lists maintenance

**Note:** The CIMT recognises that communications to internal and external stakeholders (excluding media) often requires a prompt response and therefore pre-approval by the CIMT Chair (or Comms Controller by delegation) may not always be possible and release of the communications is at the discretion of the DSM Coordinator.

**Planning/Intelligence Controller (P&I Controller) and Team**

**Planning/Intelligence Controller (P&I Controller)**

The role of the P&I Controller is to manage the gathering of information required to assist management of the incident for the CIMT. They also manage any call centre and counselling centre requirements.

The responsibilities of this role are:

- To ensure adequate training has been received that is suitable for the role.
- To establish the means to identify impacts to staff, students and faculty.
- Establish the means to report on any injured parties to CIMT.
- To set up and oversee an incident control call centre when required, to manage incoming calls and Emails.
- Consider the need for counselling for staff, students, next of kin and other relevant stakeholders and implement management activities including a counselling centre if required.
- To determine the requirement for specialist advice during incident management and sourcing suitable expertise e.g. Biosafety Manager, Chemical & Safety Advisor, Radiation & Safety Officer, Director Research Services etc. to assist CIMT.
- To ensure timely escalation to CIMT Chair of any concerns regarding staff, students and faculty, and to keep the CIMT informed of developments
- Monitor and report the insurance impacts of the CIMT and Incident Controller’s decisions.
- To ensure there is a suitable person on call in all roles within the team at all times and that the contact list for the team is up to date to support CIMT incident notification processes.
- All toolbox items remain up to date
The Planning & Intelligence Team is made up of the following members:

**Human Resources Coordinator (HR Coordinator)**
The role of the HR Coordinator is to support the actions of the CIMT such that ensure the safety and wellbeing staff is considered at all times. They also assist by providing staff information and advice on staff matters.

The responsibilities of this role are:
- To ensure adequate training has been received that is suitable for the role.
- Identifying the impacts on staff and communicating them to CIMT.
- Identification of all staff involved in the incident and establish communications with injured parties.
- Providing staff personal contact and other personal information (including next of kin contact information) to the Communications Controller and CIMT if required for communications or other purposes.
- Ensures the appropriate protocols for police notifications to next of kin of effected staff are followed. (Student next of kin is handled by the Student Coordinator)
- Provides advice on any staff, industrial relations and union issues.
- Arranges for any required counselling requirements.
- Manages any response by Safety Health & Wellbeing, including notifications to Workcover for safety incidents.

**Student Coordinator**
The role of the Student Coordinator is to ensure the safety and wellbeing of students is considered. It also assists in providing information and advice on student matters.

The responsibilities of this role are:
- Ensuring adequate training has been received that is suitable for the role.
- Identifying the impacts to students and communicating them to the CIMT.
- Identification of all students involved in the incident.
- To liaise as necessary with the Communications Controller in the development and issuance of student communications.
- Providing student contact and other information (including next of kin contact information) to the Communications Controller and CIMT if required for communications or other purposes.
- Ensures the appropriate protocols for notifications to next of kin are followed.
- Provides advice on any student issues and impacts on student bodies (eg Guild, clubs, residences etc.)
- Arranges for any counselling requirements.

**Faculty Coordinator**
The role of the Faculty Coordinator is to assist in providing information and advice on faculty, teaching, research and administration impacts arising from the event.

The responsibilities of this role are:
- To ensure adequate training has been received that is suitable for the role.
- To identify which (if any) faculty staff should attend the CIMT.
- Identifying the impacts to faculty, teaching, research and administration and communicating them to the CIMT.
- Ensures the appropriate protocols are followed for notifications to research grant and other faculty stakeholders.
Operations Controller (Ops Controller) and Team

Operations Controller (Ops Controller)
The role of the Ops Controller is to ensure a clear line of communication between the CIMT and those managing the response at the incident site. The Ops Controller liaises with the site incident controller and other command post staff.

The responsibilities of the Ops Controller are:
- To ensure adequate training has been received that is suitable for the role.
- To verify and confirm that a command post/control point has been established at the site to capture incident information and pass back to CIMT.
- To establish and maintain a direct communications line between CIMT and the Incident Controller at the site, Security and all impacted local Business Continuity Coordinators.
- To establish and maintain a direct communications line between CIMT and all impacted local Business Continuity Coordinators.
- To ensure there is a suitable person on call in all roles within the team at all times and that the contact list for the team is up to date to support CIMT incident notification processes.
- All toolbox items remain up to date.

The Operations Team is made up of the following members:

Security Coordinator
The role of the Security Coordinator is to liaise between the Incident Controller on the ground and CIMT. The role is pivotal in ensuring CIMT are well informed and respond appropriately and in a timely manner.

The responsibilities of this role are:
- To ensure adequate training has been received that is suitable for the role.
- Establishing an agreed line of communication with the Incident Controller at the site (Command Post).
- Ensure clear and prompt communication to CIMT regarding the details of the incident.

Document Control & OCA System Coordinator (Document Coordinator)
The role of the Document Coordinator is to record and track all actions taken by the CIMT. This also enables review by any required parties post incident. It includes confirming completion to the CIMT Chair. This can be undertaken manually or via the OCA System at the Document Coordinators discretion.

The responsibilities of this role are:
- To ensure adequate training has been received that is suitable for the role.
- Document control of action actions taken during CIMT meetings, action plan management and time line recording.
- Management of the CIMT OCA system during an incident.
- Assist the Gap Analysis process.

Security & Building Systems Coordinator (S&B Systems Coordinator)
The role of the S&B Systems Coordinator is:
- To ensure adequate training has been received that is suitable for the role.
- To monitor security and building systems and report concerns where identified. These include CCTV, Access Control and OCA.
- Enable OCA system access to CIMT as required.
- To provide training of the OCA system to the CIMT.
- To ensure that the list of CIMT staff (& alternates) is up to date in OCA to support CIMT incident notification processes.
Logistics Controller and Team

Logistics Controller
The role of the Logistics Controller is to oversee the actions required by Campus Management (CM) and Business Information & Technology Services (BITS) in restoring critical infrastructure to UWA. The Logistics Controller will provide information regarding critical infrastructure impacted by the incident and ensure records of the CIMT’s management of the incident are maintained (including action tracking).

The responsibilities of this role are:
- To ensure adequate training has been received that is suitable for the role.
- To establish and maintain a direct communications line between CIMT and CM/BITS responders.
- To ensure CIMT actions are tracked and reviewed to ensure all key actions are completed or outstanding actions are reported to the CIMT Chair.
- To ensure maintenance of a timeline of events to enable gap analysis to be undertaken after the closure of an incident.
- To ensure the CIMT room contains all required equipment/resources to assist in the management of an incident. This includes equipping call centre rooms run by the Internal communications Coordinator.
- To ensure there is a suitable person on call in all roles within the team at all times and that the contact list for the team is up to date to support CIMT incident notification processes.
- All toolbox items remain up to date

The Logistics Team is made up of the following members:

Facility Operations Coordinator (Facilities Ops Coordinator)
The role of Facilities Coordinator is to ensure CIMT is provided with information about impacted UWA infrastructure and strategies for it to be reinstated/restored. The role is also responsible for ensuring the CIMT Rooms are suitably equipped and maintained to manage a critical incident.

The responsibilities of this role are:
- To ensure adequate training has been received that is suitable for the role.
- To establish and maintain a direct communications line between CIMT and the CM responders.
- Maintaining hard and soft copy maps and building information in all CIMT rooms.
- Determining restoration solutions for impacted buildings and infrastructure.
- To ensure all CIMT Rooms are equipped with all required equipment/resources that assist in the management of an incident. Also to ensure the equipment is up to date and maintained appropriately (including call centre requirements).

Information Services Coordinator (IT Coordinator)
The role of the IT Coordinator is to ensure CIMT is provided with information regarding impacted UWA IT infrastructure and strategies for it to be reinstated/restored. The role is also responsible for ensuring the CIMT Rooms are suitably IT equipped with appropriate information and telecommunications technology and maintained to manage a critical incident.

The responsibilities of this role are:
- To ensure adequate training has been received that is suitable for the role.
- To establish and maintain a direct communications line between CIMT and the BITS responders.
- Providing and maintaining hard and soft copy information on all UWA IT infrastructures.
- To ensure all CIMT Rooms and call centre rooms are equipped with all required equipment/resources that assist in the management of an incident. Also to ensure the equipment is up to date and maintained appropriately.
- Determining restoration solutions for impacted buildings and infrastructure.

Business Continuity Response Coordinator
The role of the BC Response Coordinator is to identify impacts to local business units and assist impacted businesses to recover priority processes, equipment and infrastructure or respond to an incident where it is outside of CIMT direct control as determined by the CIMT Chair.

The responsibilities of this role are:
- Identification of impacts to business units priority processes, equipment and infrastructure
• Providing information on pre-planned recovery requirements for the impacted priority processes, equipment and infrastructure
• Assisting the business unit to promptly respond to the incident’s impact to priority processes, equipment and infrastructure (as per their BCP)
• Ensuring the business units coordinate their response with the CIMT

Support Roles
There are various other UWA and external support functions that will be requested to provide assistance as required and as deemed suitable by the CIMT Chair. The following provides some examples of support area's/personnel that may be called on to assist CIMT:

Risk & Legal Division - assist in provision of legal advice etc. and manage the post incident requirements – perform operational management, gap analysis, audits etc.

Insurance Advisor – Guidance on restoration actions by CIMT in relation to insurance matters

Safety, Health & Wellbeing - Provision of assistance as required and reporting to Worksafe if required.

Biological, Chemical and Radiological Safety Officers – provision of specialist advice relating to the incident and its impacts etc.

Deans, Directors, Heads of Schools, Faculty and School and Centre Managers are responsible for assisting the CIMT in managing critical incidents impacting the University and for ensuring that BCPs are activated and managed when required.

UWA Staff are expected to support the planning and recovery processes in their Business Unit and to respond to support requests from the CIMT. All staff are expected to follow the instructions of the ECO in the case of an emergency and during training exercises.
7. **Training & Testing and Maintenance of BCM Capability**
The University aims to implement and maintain a regular program of BCM training, testing and review.

7.1. **Training**

7.1.1. **Emergency Management Training**
UWA Security will ensure they have fully accredited and trained staff undertaking the security functions.

UWA Safety, Health & Wellbeing will ensure that every UWA building has suitably trained Fire Wardens and First-Aid Officers.

Safety & Health and UWA Security will be responsible for ensuring the suitability of training and testing for the Emergency Control Organisation and other specialists.


7.1.2. **CIMT Training**
CIMT training will be provided to key CIMT members by Risk & Legal Division. The training will cover the key responsibilities for each role and how the OCA system works to assist CIMT in managing an incident.

The training will consist of:
- Induction training upon appointment for CIMT members.
- Exercise training for the Critical Incident Management Team and relevant stakeholders.

UWA Leadership and other stakeholders of the CIM process will receive CIMT awareness training to assist them to understand the role of the CIMT.

7.1.3. **BCP Training**
To improve awareness of the BCM program and Business Unit BCPs, the following training will be provided by Risk & Legal Division:
- Induction training upon appointment for BRT members.
- Exercise training for selected management and BRT for each Business Unit and selected stakeholders (e.g. Campus Management).
- Awareness training session for general staff.

7.2. **Testing**
Risk & Legal Division will implement a cyclical testing regime to provide confidence that the CIMT & Local Business Recovery Teams will meet performance expectations.

7.2.1. **Emergency Control Organisation Testing**
The testing of the Emergency Incident Management requirements is the responsibility of UWA Safety, Health & Wellbeing.

Refer to their website for more information: [http://www.safety.uwa.edu.au/incidents-injuries-emergency/procedures](http://www.safety.uwa.edu.au/incidents-injuries-emergency/procedures)

7.2.2. **Critical Incident Management Testing**
It is vital to ensure that the CIMT has the tools and training to manage incidents critical to UWA’s operations and reputation. The training will be undertaken by Risk & Legal Division.

A 5 year testing cycle will include:
- **Within years 1 to 4:** a desktop simulation (scenario) test. This approach requires CIMT and key stakeholders to discuss the application of the CIMT Manual for responding to a presented hypothetical major disruptive event scenario. The activity does not require the activation and mobilisation of any associated resources or personnel.
- **In year 5:** an actual activation scenario facilitated as necessary. This test may involve emergency services and other relevant third parties.
The outcomes of the test will be integrated into the CIMT Manual, processes and any other emergency response documentation by the UWA BC Manager. Updated versions are to be distributed to all required parties.

The CIMT and key stakeholders are exempt from the annual testing activities where the following occurs:

- A large scale critical incident has been managed within the last 12 months (with associated debriefing processes);
- An exemption is obtained that is approved by the Assoc. Director of Legal & Risk, giving the reasons why the training or test cannot be completed and giving a timeframe for the training / testing to occur. This shall be done in consultation with the Senior Deputy Vice Chancellor.

### 7.2.3. BIA & BCP Testing

The testing of recovery strategies put into place by Business Units will require testing at least over a five year cycle to ensure the BCP is current and reliable.

During each 5 year cycle, all Business Units are to review their BIA’s & BCPs (where one exists) at least once to ensure there are no changes to indicated process requirements, and ensure any new processes are input and assessed.

### 7.2.3.1. High Priority BCPs

The following is specifically designed to cater to Business Units with processes assessed by the Assoc. Director Risk & Legal, Strategic Risk Manager and the BC Manager as being of the highest priority to UWA.

A five-year testing cycle that includes:

- **Within years 1 to 4:** a desktop simulation (scenario) test approach for selected Business Units. This approach requires participants to discuss the application of BCPs for responding to a presented hypothetical major disruptive event scenario. The activity does not require the activation and mobilisation of any associated resources or personnel.

- **In year 5:** a unit rehearsal - restricted plan activation and mobilisation activity. Typically, selected priority processes, equipment and infrastructure would be required to mobilise resources to respond to a presented major disruptive event scenario. This may also involve utilisation of an alternate site.

The outcomes of these reviews and testing activities will be integrated into the existing BCPs, and any other emergency response documentation by the Business Recovery Coordinator and reviewed by the BC Manager. Updated versions are to be distributed to required parties.

### 7.3. Review and Maintenance

**7.3.1. Business Continuity Management Framework**

The Risk & Legal Division is responsible for ensuring that a review of this BCM Framework is conducted on a five yearly cycle.

**7.3.2. Critical Incident Response Plan**

The CIRP must be reviewed by Risk & Legal Division within 90 days of any major operational or system changes that may have a material effect on the recovery actions to be undertaken or documented in the plan e.g. change to security software (OCA), operations, change to legislation/compliance, restructure, etc.

**7.3.3. Business Impact Analysis (BIAs) and Business Continuity Plans (BCPs)**

The BIA and BCP must be reviewed by the Business Unit for possible updating within 120 days of any major operational or system changes that will have a material effect on the recovery strategy of a Business Unit (change to operations, change to legislation/compliance, restructure etc).
8. **Appendices:**

8.1. **Definitions**

Note: This diagram represents the relationship between a number of definitions set out below and discussed in more detail in Section 2.

1. **Business Continuity Management (BCM):** a holistic process managing the University’s activities to ensure effective management of a material disruption, and the maintenance and restoration of priority processes, equipment and infrastructure with minimal impact to staff, students and the general community. It is the management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity. It incorporates the Business Continuity Management Framework.

2. **Business Continuity Management Framework:** the framework describes the structure, process and resourcing that enables the University to manage incidents and develop continuity strategies and plans.

3. **Business Continuity Planning (BCP):** is a set of documents with instructions and procedures to enable UWA Business Units to respond to accidents, disasters, emergencies and threats to ensure minimal disruption to priority processes, equipment &/or infrastructure. It enables a business to recover operations until normal University activities can be restored.

4. **Business Impact Analysis (BIA):** is a detailed risk analysis that examines the nature and extent of disruptions and the likelihood of the resulting consequences. A BIA involves the consideration of the University’s or Business Unit’s functions, people, processes, infrastructure, resources, information, interdependencies and the nature and extent of capability loss over time.

5. **Business Recovery Team (BRT):** Specific members of a Business Unit that perform required actions to manage the business recovery activities (as contained in the BCP).

6. **Critical Incident** is defined as a sudden event or series of events that seriously threatens the University’s people, animals, assets, operations, environment, long term prospects and reputation. It may be natural (e.g. flood, bush fire, earthquake), accidental (e.g. fire, contamination), commercial (e.g. loss of supply of critical services) or wilful (e.g. sabotage, vandalism, arson, terrorism). These incidents require an “institutional response”.

   Note: The Critical Incident Management Team (CIMT) Chair decides if an incident is a critical incident.

7. **Critical Incident Management (CIM):** is the initial management of a disruption impacting one or more UWA Business Units which could lead to reputational damage or the failure to meet UWA’s objectives. CIM is completed when the CIMT Chair formally declares that the immediate requirements of the incident are resolved. The process for management will then move to activation of the local business unit’s BCP, or returning directly to normal University activities.

   Critical incidents are to be centrally managed by the nominated Critical Incident Management Team (CIMT). They will engage representatives from UWA Business Units or key stakeholders as the need arises.

8. **Critical Incident Response Plan (CIRP):** is a set of documents with instructions and procedures to enable the Critical Incident Management Team to respond to accidents, disasters, emergencies and threats to UWA people, animals, reputation and assets.

9. **Emergency:** An emergency is a situation that poses an immediate risk to health, life, property or the environment. Most emergencies require urgent intervention to prevent a worsening of the situation.
10. **Emergency Incident Management**: is the management of an incident requiring an immediate response from the UWA Emergency Control Organisation, UWA Security and or Emergency Services (Fire, Ambulance, Police etc.). The management of an emergency may require one or more specialist response agents/services, and be incident controlled by UWA Security, unless the external Emergency Services agency is required.

*Note:* Not all emergencies become Critical incidents e.g. a broken leg may require Emergency Services (ambulance) but not an institutional response.

11. **Emergency Control Organisation (ECO)**: is comprised of the trained Fire Wardens & First Aid Officers assigned to specific buildings, UWA Security and UWA Safety, Health & Wellbeing. They are responsible for implementing the emergency procedures as prescribed in the Emergency Plan and Procedures.

During business hours Monday to Friday (excluding University Holidays) it is controlled by UWA Security (Campus Emergency Coordinator, Communications Officer, Emergency Response Officer), First Aid Officers and Specialists (e.g. Chemists), Building and Area Wardens. Outside of these times, the Security Controller will assume the role of the Emergency Response Officer (also known as Incident Controller) and will be responsible for coordinating the initial response to an emergency. At UWA these groups are also represented on the CIMT due to the ongoing impact of most emergencies.

12. **Incident Controller** – is the person in charge of incident response activities. This will be the most competent UWA staff member that is on the scene until management can be handed over to an Emergency Services, ECO, CIMT or Business Unit (for local incident management) representative.

13. **Local Incident Management**: is the management of non-material disruptions by the local Business Unit and may result in activation of their BCP if priority processes, equipment and infrastructure are impacted. Activation of the CIMT is not required (CIMT will notify local management if they are to manage the incident).

14. **Maximum Acceptable Outage (MAO)**: Maximum period of time that the University can tolerate the disruption of a priority business process, equipment or infrastructure. Disruption may include the discontinuance of an activity, or the inability to perform it to an acceptable quality or with sufficient reliability or failure of a controlled environment/system or piece of equipment.

15. **Priority Processes**: are those processes that are critical for the successful operation of the business or University as a whole, and, if not performed for a time period longer than the identified maximum tolerable outage (MAO), would lead to a risk with a consequence of Major or greater (refer to UWA’s Risk Management Framework).

16. **Priority Equipment**: refers to any equipment, machinery or devices that if impacted by an incident and not operating for a time period longer than the maximum acceptable outage (MAO), would lead to a risk with a consequence of Major or greater (refer to UWA’s Risk Management Framework).

17. **Priority Infrastructure**: refers to any core service or structural item provided by UWA that is fundamental to core operations (teaching & research). If there is a failure to provide the service or structural item it could lead to a risk with a consequence of Major or greater (refer to UWA’s Risk Management Framework) it is to be regarded as a priority.

18. **University Activities**: the University’s day to day business processes and operations, i.e. teaching and research activities, community connection activities and support services.

19. **Risk assessment** is the overall process of risk identification, risk analysis and risk evaluation.

20. **Stakeholders** are those people and organisations that may be engaged to assist in or be impacted by, a decision or activity.
8.2. Business Continuity Planning Guide - Planning Considerations

8.2.1. Recovery Strategies

Recovery strategies may take many forms. Regardless of the type of incident, there are the following general scenarios to consider:

- If the incident only impacts the individual business unit
- If it is a UWA wide incident.

The latter consideration is relevant because other impacted Business Units may wish to relocate to the same alternate site.

There may be different recovery strategies depending on the nature of the incident and these will be documented in the BCP. For instance:

- A process may be able to be actioned from an alternate location such as working from home or another UWA building. Both have different enabling actions e.g. working from home requires remote access.
- A Business Unit may have research materials in a -20°C freezer that must be relocated if power fails. If it is a local impact, you may plan to move the contents to another freezer in the building next door. However if power to the campus is lost, you need to bring portable power sources to the freezer.
- If core systems are lost, strategies may be to defer the process, use a manual workaround process, or engage an external vendor.

There are some standard scenarios that would apply to all Business Units. There may also be some that are unique to the business unit. For instance if a Business Unit relies heavily on a vendor to provide goods or services, what recovery strategy is in place if they fail to deliver?

The UWA BIA template includes examples of the following scenarios to assist the development of the BCPs:

<table>
<thead>
<tr>
<th>SCENARIO</th>
<th>DESCRIPTION</th>
<th>POSSIBLE CAUSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Localised denial of access to building, floors and precinct</td>
<td>Assets inside the building are not lost and cannot be accessed.</td>
<td>Students/teachers on strike, storm damage, Emergency Services stop access</td>
</tr>
<tr>
<td>Loss of workplace due to fire, flood etc</td>
<td>Permanent loss of non-electronic records, research materials, equipment, IT infrastructure, inability to undertake lectures.</td>
<td>Natural disaster, deliberate act (arson, explosion), accident (fire, flood)</td>
</tr>
<tr>
<td>Pandemic/extended shortage of staff (high volume)</td>
<td>Inability to maintain processes due to insufficient staff numbers.</td>
<td>Pandemic, epidemic, extended strike action by staff</td>
</tr>
<tr>
<td>Loss of IT Systems</td>
<td>Inability to maintain processes or use equipment due to failure of key IT systems.</td>
<td>Deliberate act (hacking etc.), server room fire</td>
</tr>
<tr>
<td>Loss of utilities (temporary loss of electricity, gas, solar etc)</td>
<td>Temperature controlled environments lose integrity and research lost. Specialised machinery ceases due to uncontrolled shutdown.</td>
<td>Construction cuts through a gas pipe, aged infrastructure, power to UWA fails.</td>
</tr>
<tr>
<td>UWA wide incident</td>
<td>Incident impact is across multiple Business Units and/or impacting multiple priorities</td>
<td>Gas leak, biohazard etc.</td>
</tr>
</tbody>
</table>
There may be other recovery strategies specific to the business unit’s needs, or there may be a combination of solutions. For instance a process may need to be relocated and staff may need to work overtime to complete the priority process once set up, but the business may have rare documents, artefacts or research materials that need to be recovered.

Example recovery strategies and a description are listed below:

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defer all activity</td>
<td>Place the process on hold and notify required stakeholders of the inability to complete the activity. Ensure equipment is in a safe hibernation state.</td>
</tr>
<tr>
<td>Restore environmental conditions</td>
<td>Obtain and set up portable generators to provide temporary power to equipment until restored or a long term solution is determined.</td>
</tr>
<tr>
<td>Relocate to alternate site and resume</td>
<td>Send required staff to another UWA location to complete the activity. Provision with alternate site access, equipment etc. as required</td>
</tr>
<tr>
<td>Work from home</td>
<td>Send required staff home to complete the activity, arrange for provision of equipment/access etc. as required</td>
</tr>
<tr>
<td>Activate manual work-around process</td>
<td>Action the activity using a manual procedure. For instance, input data to an Excel spreadsheet instead of loading to a system. The data can then be uploaded or entered when systems are restored.</td>
</tr>
<tr>
<td>Buddy-up at alternate location</td>
<td>Send required staff to sit at a desk with another staff member to share the workspace and facilities. This may be required if there is limited workstations for the process.</td>
</tr>
<tr>
<td>When resumed - work rotational shift</td>
<td>To catch up on workloads previously deferred, have staff work around the clock to complete. Ensure after hours security and building access is provided.</td>
</tr>
<tr>
<td>Undertake process as per usual</td>
<td>The incident may not impact this particular priority process and so the Business Unit can continue to operate as per usual. For instance, in a system failure incident where the system isn’t used for that particular process.</td>
</tr>
<tr>
<td>Prioritise processes and action</td>
<td>If there are limited resources, staff are diverted to focus on the priority processes.</td>
</tr>
</tbody>
</table>

**Relocation to Alternate Site Strategy**

If a Business Unit can no longer access their usual workplace, alternate sites for relocation should be considered.

The alternate site should be compliant with the University’s Work, Health & Safety and other procedures. Formal arrangements may be required e.g. formal agreement or letter of understanding to facilitate access. This will be particularly important for external arrangements.

Options considered could include:

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UWA site on-campus</td>
<td>move in with others of same/different Business Unit or operate outside normal business hours</td>
</tr>
<tr>
<td>UWA site off-campus</td>
<td>move in with others of same/different Business Unit - University owned</td>
</tr>
<tr>
<td>External site off-campus</td>
<td>working at home or renting space, or other WA University campus – third party owned</td>
</tr>
</tbody>
</table>

**Time of Year**

Different processes may have different priorities at different key points of the year. For instance early in each semester examination processes are Priority 3. However if a specialised exam venue experiences a power outage just prior to exams, the examination process moves up to Priority 1 and a BCP may be needed to relocate it.

Processes that are regarded as Priority 1 at key points of the University calendar should be indicated as Priority 1 in the BIA, and planned for in the BCP. Should an incident arise outside of these key times, it can then be disregarded as appropriate.
Staff Requirements
It is important to consider the minimum number of staff required to carry out the priority processes. This should be the absolute minimum given the recovery strategy is to only undertake the priority process requirements.

This is particularly important during a UWA wide incident or a pandemic scenario, as there could be limited ability to accommodate people at the recovery site and/or limited people to undertake them. Your staff may also be required to assist in other recovery activities.

Another consideration may be to outsource a process for the period of disruption.

Single Person Dependency
The specialist skills required to undertake the recovery actions for the priority processes, equipment and infrastructure may be limited. The Business Unit may need to document processes, practice multi-skilling, or find a suitable outsource arrangement so the single person dependency is avoided.

Specialist Equipment/Resources
It will be important to note whether any specialised equipment or resources are required for a priority process. Key questions to ask are:

- Can you recover the item from the work site?
- Can a replacement be found in a short timeframe? Is it cost effective?
- Is there another solution i.e. to send the people and processes to another location (even another University)? Has it been confirmed that it will be possible to do so?

Internal & External Dependencies
Where there is reliance on another UWA Business Unit for the provision of services, provision should be made in the BCP to ensure they can be contacted and include the relevant actions relating to it in the process checklist/s. The Business Unit must ensure they engage with the impacting Business Unit to agree to the actions to be taken.

This may also be the case for external service providers. For instance the BCP may note how the supplier’s agreement allows UWA to request priority service provision. Alternate suppliers should also be noted, and their contact details.

Communications
Communications strategies should be considered. Identify who needs to be informed of the incident both internally and externally. If there are vendors that supply a priority process, the Business Unit must contact them to cancel, redirect or amend the delivery/service provision.

The method and frequency of ongoing communication needs also to be considered and pre-planning may assist to ensure all required parties are accommodated.

Costs
The costs of the recovery strategy also need consideration. If costs to restore the process significantly outweigh the value of the process, an alternate strategy should be considered or the priority of the process re-assessed.

Full Restoration
Establishing a BCP that assists a Business Unit to restore priority processes, equipment and infrastructure is essential, but it is also important to consider the processes required to return to normal operations and reverse the actions taken where required. The return to normal operations process is particularly important when it involves moving people, animals and equipment.

The BCP should outline the key elements of recovering operations, ensuring the checklist includes the steps to reverse any actions taken. For instance, to ensure no loss of research specimens stored in freezers occurs, the materials may have been transferred to an alternate site. Before moving it back, the BCP may need to stipulate that the freezer it is returning to must be at a specific temperature before the materials are returned.

This sounds obvious, but in times of stress it is easy to forget some basics, or to assume someone else is doing the task.
### 8.3. Document Information

<table>
<thead>
<tr>
<th>Document No: To be provided when approved</th>
<th>Approving body or position:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Senior Deputy Vice Chancellor; or</td>
</tr>
<tr>
<td></td>
<td>2. Assoc. Director of Legal &amp; Risk</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date document approved as final version:</th>
<th>Date this version of document approved:</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A as new document</td>
<td>To be provided when doc approved</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date document to be reviewed:</th>
<th>Contact position:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020</td>
<td>Assoc. Director of Legal &amp; Risk</td>
</tr>
<tr>
<td></td>
<td>Business Continuity Manager</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TRIM File No: To be provided when doc approved and uploaded</th>
<th>Related Policies or legislation:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>ISO22301</strong> – Business Continuity Management Systems - a globally accepted standard for BCM systems</td>
</tr>
<tr>
<td></td>
<td><strong>AS/NZS 5050:2010</strong>, the standard that guides the application of ISO 31000 to disruption related risks.</td>
</tr>
<tr>
<td></td>
<td><strong>ISO 31000</strong> – Risk Management.</td>
</tr>
<tr>
<td></td>
<td>The University of Western Australia Business Continuity Management Policy.</td>
</tr>
</tbody>
</table>

### References

- AS/NZS5050:2010 Business Continuity- managing disruption-related risk
- ISO22301 – Business Continuity Management Systems
- ISO31000: Risk Management – principles and guidelines
- The University of Western Australia: Risk Management Policy (UP12/1).