## TABLE OF CONTENTS

1. Introduction ............................................................................................................................................... 3  
   1.1. Document Version Control .................................................................................................................. 3  
   1.2. Terminology ......................................................................................................................................... 3  
   1.3. Purpose and Scope of this Framework ................................................................................................. 4  
   1.4. Structure of this Document ................................................................................................................ 5  
   1.5. What is Business Continuity Management? ....................................................................................... 5  
   1.6. Business Continuity Policy Statement ............................................................................................... 8  
   1.7. Relationship to the Risk Management Policy ..................................................................................... 8  
   1.8. Relationship to Other Policies and Procedures ................................................................................... 8  
2. Business Continuity Management Roles and Responsibilities ................................................................ 9  
3. Notification and Activation Processes .................................................................................................. 10  
4. Existing Business Continuity Arrangements ........................................................................................ 11  
   4.1. Departments with Business Continuity Plans .................................................................................... 11  
   4.2. Continuity Arrangement Design ....................................................................................................... 11  
   4.3. Alternative Site Strategy .................................................................................................................... 12  
5. Summary of Critical Functions ............................................................................................................... 12  
6. Building and Embedding a Business Continuity Management Culture .............................................. 13  
   6.1. General ........................................................................................................................................... 13  
   6.2. Outcomes ......................................................................................................................................... 14  
7. Training, Testing and Maintenance of Business Continuity Arrangements ...................................... 15  
   7.1. Training ......................................................................................................................................... 15  
   7.2. Testing ........................................................................................................................................ 15  
   7.3. Review and Maintenance .................................................................................................................. 16  
8. References ........................................................................................................................................... 17
1. Introduction

1.1. Document Version Control

<table>
<thead>
<tr>
<th>Version No</th>
<th>Description</th>
<th>Author</th>
<th>Reviewed by</th>
<th>Issue date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Draft for consultation</td>
<td>A Walker</td>
<td></td>
<td>20/11/2009</td>
</tr>
<tr>
<td>0.2</td>
<td>Aligned for consistency with Emergency Management Framework</td>
<td>A Walker</td>
<td>C Schraders</td>
<td>20/09/2011</td>
</tr>
<tr>
<td>0.2</td>
<td>Aligned for consistency with AS/NZS5050:2010</td>
<td>A Walker</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Final Approved by SLT 12/11/243</td>
<td>A Walker</td>
<td></td>
<td>Dec 2012</td>
</tr>
</tbody>
</table>

1.2. Terminology

**Business Continuity** is “the uninterrupted availability of all key resources supporting essential business functions” (Australian National Audit Office, 2000).

**Business Continuity Plan (BCP)** are a collection of procedures and information that is developed, compiled and maintained in readiness for use in the event of an emergency or disaster.

**Critical functions** are those functions and/or processes that are critical for the survival of the organisation, 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 Moderate or greater (refer to Massey...
University’s Risk Management Framework for more information). For simplicity, critical functions listed in this Framework are those functions with a maximum tolerable downtime (MTDT) of two weeks (10 working days) or less.

Critical user refers to a person, department or organisation that relies on the particular service function or application for most or all of their usual work or study functions.

Department refer to the business unit for which Business Continuity Plan applies. In this Framework document, Department means any sub-set of the University, including but not limited to: Sections / Divisions / Colleges / Institutes / Schools / business groups.

Information Technology Disaster Recovery Plan (IT DRP) refers to the plan and arrangements for restoring information technology assets following a technology interruption. Arrangements may include business continuity arrangements being activated at alternate production facilities.

Major disruptive event may be Natural (e.g. flood, hurricane, earthquake), Accidental (e.g. fire, contamination), Commercial (e.g. loss of supply of critical services) or Wilful (e.g. sabotage, vandalism, arson, terrorism).

NOTES: 1) Associated terms: “event”, “emergency event”.

2) In Massey University’s emergency management arrangements, the terms “event” and “emergency event” have the same meaning as “major disruptive event”.

Maximum tolerable outage (MAO) Maximum Acceptable Outage (MAO): Maximum period of time that an organisation can tolerate the disruption of a critical business function. Disruption may include both the discontinuance of an activity, or the inability to perform it to an acceptable quality or with sufficient reliability. Associated terms “Maximum tolerable outage” or “maximum tolerable period of disruption”

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

Stakeholders are those people and organisations that may affect, or be affected by, or perceive themselves to be affected by, a decision or activity.

Sub-Plan refers to any additional plan, procedure, Standard Operating Procedure (SOP) or similar document, related to emergency response or business continuity within the University.

1.3. Purpose and Scope of this Framework

This Business Continuity Management (BCM) Framework is designed to assist management and staff of Massey University to implement BCM within the organisation and to assist in familiarising new managers and staff where necessary.

This framework applies to all Massey University staff who are responsible for the establishment, implementation, or maintenance of the University’s Business Continuity Management (BCM) programme.
Massey University’s BCM programme applies to all University operations/functions, regardless of the location in which they are undertaken.

The framework does not include the operations/functions of the University’s controlled entities which are expected to maintain their own BCM programmes which is aligned to good practice.

The information within this BCM Framework serves to provide guidance to University management during an interruption to University operations that is longer than tolerable.

This framework does not include specific requirements and strategies for critical functions; these are detailed in the specific College/Campus/Division BCPs.

1.4. Structure of this Document
This framework provides an overview of Massey University’s approach to Business Continuity Management (BCM).

This section outlines the aim and scope of the Framework and relevant documents the University has in place to support the BCM programme as well as documents that are to be utilised should a major disruptive event affect the University’s operations.

Section 2 outlines the responsibilities of particular University stakeholders in establishing, maintaining and implementing the BCM programme.

Section 3 outlines the Notification and Activation process for Departmental Business Continuity Plans (BCPs).

Section 4 lists the business continuity arrangements that already exist within Massey University.

Section 5 summarises the University’s critical functions which provides an overview of the priority services which need to be restored in the first instance following an event. The basis for determining criticality within each department is any function that has a maximum disruptive period of two weeks (10 working days) or less.

Section 6 contains guidelines for building and embedding a BCM culture within the University.

Section 7 contains guidelines on:
- BCM training
- BCM testing
- The review and maintenance of BCPs and the BCM Framework.

1.5. What is Business Continuity Management?
The objective of Massey University’s BCM programme is to promote the continuity and/or rapid recovery of critical services/functions required to support the core business of the University.

The Business Continuity Policy states the following as Massey University’s Business Continuity Aim:

To safeguard our reputation and public image ...
by using best endeavours to meet the needs of staff, students, the wider community and other critical stakeholders ...

through ensuring that business critical teaching and research outcomes are not compromised by a major disruptive event.

BCM is a continuous improvement process of establishing and maintaining Business Continuity Plans (BCPs) and other measures in order to respond to and recover from disruptions that threaten key resources, locations and functions. Collectively these measures are referred to as the University’s BCM capability. This capability contributes to the University’s Emergency Management arrangements; collectively they comprise four components of response and recovery:

- **Emergency Response** – the immediate response to an event with a focus on ensuring the safety of people followed by the protection of assets (refer to the Emergency Management Policy and the Massey University Strategic Emergency Management Framework for more information);
- **Crisis Communications** – (refer to the Crisis Communications Plan for more information);
- **Business Continuity (including IT Disaster Recovery)** – the process of restoring critical elements of University services and functions within the University’s core business processes;
- **Holistic Recovery** – the broad activities required to restart, rebuild and regenerate the affected community, not just the restart of business operations.

The relationship between these four components of Massey University’s Emergency Management and BCM capability is outlined in the diagram below.

**Figure 1: The Relationship between Business Continuity Management, Emergency Management and IT Disaster Recovery.**
1.6. Business Continuity Policy Statement

Through the adoption of Business Continuity Management best practices Massey University will achieve its business continuity aim of safeguarding our reputation and public image in order to achieve the goals and objectives stated in The Road to 2020 strategy. This will occur by using best endeavours to meet the needs of staff, students, the wider community, and other critical stakeholders, through ensuring that business-critical teaching and research outcomes are not compromised by a major disruptive event.

The Business Continuity Policy forms part of the risk management framework at Massey University, and is aligned to AS/NZS5050:2010 Business Continuity – Managing disruption-related risk

1.7. Relationship to the Risk Management Policy

Business Continuity Management supports Massey University’s Risk Management Policy and provides a means of mitigating certain risks should they occur and impact a Campus, business processes, business operations or IT systems. BCM provides plans to minimise the impacts and allow the University’s processes to recover from the incident in a planned manner.

BCM also supports the University’s Emergency Management arrangements, and more specifically, BCPs can be activated during or immediately after an emergency event that is being managed in accordance with the University’s Emergency Response Plans.

1.8. Relationship to Other Policies and Procedures

The following policies and procedures are relevant to either preparing a BCP or for the implementation of BCM within the University:

- Risk Management Policy
- Risk Management Framework
- Risk Registers
- Emergency Management Policy
- Massey University Strategic Emergency Management Framework
- University Emergency Response Plan
- Crisis Communications Plan
- Campus Emergency Response Plans
- Business Continuity Management Policy
- Business Continuity Management Framework (this document)
- Guidelines for the development of Business Impact Analyses
- Departmental Business Continuity Plan Template
- BCM Training Modules
- BCM Testing and Exercising Plan
- IT Disaster Recovery Plan
- College/Region/Division Business Continuity Plans
All departmental BCPs shall include:

- Introduction (aim and scope)
- Summary of critical functions including the maximum tolerable downtime (MTDT) for each function
- Continuity arrangements for critical functions
- Contact lists
- Outline of testing/exercising/training/review guidelines
- Document control information
- Resource requirements.

2. Business Continuity Management Roles and Responsibilities

Within the University’s BCM programme, the following University stakeholders play an important role:

**University Council**
The University Council sets the policy for BCM across the University.

**Audit and Risk Committee**
The Committee advises Council in relation to the appropriateness of the University’s BCM Framework, including the BCM Policy. It is responsible for assessing the effectiveness and overseeing the maintenance of the BCM programme.

**Risk Management Office**
The Risk Management Office is responsible to the Council via the Audit and Risk Committee. The Office is responsible for implementing the University’s BCM policy including the review, development, maintenance and testing of BCPs.

**Plan Sponsors**
AVCs/PVCs/DVCs are the Sponsor of all BCPs that sit within their College or Section. Plan Sponsors are responsible for providing guidance and support for the BCP and ensuring a BCM culture.

**Plan Owners**
Department heads are appointed as Business Continuity Plan Owners. It is their responsibility (with the assistance of the Risk Management Office) to ensure that all critical functions under their responsibility are covered by their department’s BCP and that the BCP is maintained and reviewed in accordance with the Business Continuity Policy. The Plan Owners report to the Plan Sponsor.

**Function Owners**
Each critical function noted within the departmental BCP has an appointed Function Owner. This Function Owner is responsible for the implementation of continuity arrangements for the specific critical function/s should it be interrupted.
3. Notification and Activation Processes

There are two main scenarios to consider:

1. An event occurs but departments do not immediately know that their functions and processes have been, or will be, interrupted. Examples include:
   - An event occurs outside working hours which causes loss of physical access to areas of the Campus, e.g. a storm causes a tree to fall through the roof of a building.
   - An event occurs that has an immediate impact on a small area of the Campus, and has the potential to expand to impact other parts of the Campus, e.g. flooding.

2. An event occurs and departments immediately know that their functions and processes have been interrupted, e.g. a power cut.

In both situations the notification and activation processes are the same; however, the size and level of complexity of the event will determine which plans are activated.

![Diagram showing activation and notification processes.]

*Figure 2: Activation and notification processes.*
4. Existing Business Continuity Arrangements

4.1. Departments with Business Continuity Plans

Business Continuity arrangements have been, or are in the process of being, developed for departments that are responsible for critical functions that have a maximum tolerable downtime (MTDT) of two weeks (10 working days) or less. These Business Continuity arrangements are documented in Departmental BCPs for each of these departments.

<table>
<thead>
<tr>
<th>Department</th>
<th>Plan Sponsor</th>
<th>Plan Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student Management (NSATS)</td>
<td>AVC Academic and International</td>
<td>Director – Student Administration</td>
</tr>
<tr>
<td>Research Management Services</td>
<td>AVC Research and Enterprise</td>
<td>Director – Research Management Services</td>
</tr>
<tr>
<td>External Relations</td>
<td>AVC External Relations</td>
<td>Director - Communications</td>
</tr>
<tr>
<td>Teaching and Learning (Stream)</td>
<td>AVC Academic and International</td>
<td>Education Technology Manager</td>
</tr>
<tr>
<td>Library</td>
<td>AVC Academic and International</td>
<td>University Librarian</td>
</tr>
<tr>
<td>Finance Operations</td>
<td>AVC Finance, Strategy and IT</td>
<td>Director – Finance and Asset Management</td>
</tr>
<tr>
<td>Facilities Management</td>
<td>AVC and University Registrar</td>
<td>Facilities Directors</td>
</tr>
<tr>
<td>Student Life</td>
<td>AVC and University Registrar</td>
<td>Campus Registrars</td>
</tr>
<tr>
<td>Payroll and HR</td>
<td>AVC People and Organisational</td>
<td>HR Services Manager</td>
</tr>
<tr>
<td>IT services</td>
<td>AVC Finance, Strategy and IT</td>
<td>CIO</td>
</tr>
</tbody>
</table>

4.2. Continuity Arrangement Design

Continuity arrangement design aims to provide a level of functionality and service which allows (at least) all ‘critical users’ of the recovered service or application across the University to perform their ‘critical functions’ with little or no special training; little or no change to their local workstation and local network configuration; and little or no reduction to their general productivity.

While this is an optimistic view to take, it makes sense to aim for the best solutions possible, within the constraints that exist.
4.3. Alternative Site Strategy

In the case of events that result in the failure of the room or building that houses the affected function and/or supporting systems and services, continuity options have been developed to utilise alternative sites. Three alternative site options are generally considered in the BCPs which are:

- Alternative site on-Campus
- Alternative site off-Campus (University owned)
- Alternative site off-Campus (may be third-party owned).

These options are to be evaluated by the Plan Owner as part of their continuity strategy at the time of the major disruptive event, and are to be facilitated in consultation with Facilities Management and, where applicable, the relevant Emergency Management Team.

For specific alternative site continuity arrangements, refer to individual BCPs for details.

5. Summary of Critical Functions

This table lists all functions within the University’s Departments that have been identified as ‘critical’. The Maximum Tolerable Downtime (MTDT) for these critical functions is two weeks (10 working days) or less.

<table>
<thead>
<tr>
<th>Department</th>
<th>Plan owner</th>
<th>MTDT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communications (including Contact Centre)</td>
<td>AVC – External Relations</td>
<td>1 hour</td>
</tr>
<tr>
<td>Security services</td>
<td>Facilities Directors</td>
<td>1 hour</td>
</tr>
<tr>
<td>Insurance management</td>
<td>Director – Finance and Asset Management</td>
<td>1 hour</td>
</tr>
<tr>
<td>Special needs (e.g. animal welfare, student health and counselling services, student residential services)</td>
<td>Various managers</td>
<td>1 hour</td>
</tr>
<tr>
<td>IT Operations</td>
<td>CIO</td>
<td>1 hours</td>
</tr>
<tr>
<td>PG Scholarship management process</td>
<td>Dean – Graduate Research School</td>
<td>0.5 days</td>
</tr>
<tr>
<td>Bio security / HASNO / Radiation Safety process</td>
<td>PVCs</td>
<td>0.5 days</td>
</tr>
<tr>
<td>Enrolment processing</td>
<td>AVC and University Registrar</td>
<td>0.5 days</td>
</tr>
<tr>
<td>Emergency management and BCP processes</td>
<td>SLT and Management</td>
<td>0.5 days</td>
</tr>
<tr>
<td>E-learning (Stream) operation</td>
<td>AVC – Academic and International</td>
<td>1 day</td>
</tr>
<tr>
<td>Timetabling service</td>
<td>Facilities Directors</td>
<td>1 day</td>
</tr>
<tr>
<td>Payroll processing</td>
<td>AVC – People and Organisational Development</td>
<td>1 day</td>
</tr>
<tr>
<td>Teaching activities (face-to-face)</td>
<td>Relevant PVCs</td>
<td>2 days</td>
</tr>
<tr>
<td>Postgraduate enrolment process</td>
<td>Student Management and PVCs</td>
<td>2 days</td>
</tr>
</tbody>
</table>
### 6. Building and Embedding a Business Continuity Management Culture

#### 6.1. General

Building and embedding a BCM culture within Massey University is critical for the establishment of an effective and robust business continuity programme. Implementing cultural change is a challenging and continuous process and its success within the University is primarily dependent upon the following:

- **a)** BCM becoming an integral part of the University’s strategic and day-to-day management ethos;
- **b)** Education, awareness training and participation being used to effect cultural change (merely documenting a BCM strategy and plan represents a narrow and limited method of developing a BCM culture);
- **c)** Preparation and delivery of a programme to create organisational awareness and enhance the skills, knowledge and experience required to implement, maintain, manage and execute BCM;
- **d)** Communication of the Business Continuity Policy and the visible proactive support from the University’s executive, senior and middle management;
- **e)** Ownership of BCM by the various Departments where operational risk originates and resides (not just within Facilities Management and/or IT Services);

---

<table>
<thead>
<tr>
<th>Department</th>
<th>Plan owner</th>
<th>MTDT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key research infrastructure (to be further evaluated)</td>
<td>Relevant PVCs</td>
<td>2 days</td>
</tr>
<tr>
<td>Library Services (online and books)</td>
<td>University Librarian</td>
<td>2 days</td>
</tr>
<tr>
<td>Relationship management with key stakeholders</td>
<td>VC and SLT</td>
<td>2 days</td>
</tr>
<tr>
<td>Marketing and Communications service</td>
<td>AVC – External Relations</td>
<td>2 days</td>
</tr>
<tr>
<td>Treasury function</td>
<td>Director – Finance and Asset Management</td>
<td>2 days</td>
</tr>
<tr>
<td>Finance One (including Procurement)</td>
<td>Director – Finance and Asset Management</td>
<td>3 days</td>
</tr>
<tr>
<td>PG Assessment and Completion process</td>
<td>Dean – Graduate Research School</td>
<td>1 week</td>
</tr>
<tr>
<td>PG Examinations and final assessments</td>
<td>Dean – Graduate Research School</td>
<td>1 week</td>
</tr>
<tr>
<td>RIMS operation</td>
<td>Director – Research Management Services</td>
<td>1 week</td>
</tr>
<tr>
<td>Student recruitment</td>
<td>AVC – External Relations</td>
<td>1 week</td>
</tr>
<tr>
<td>Printery processing and despatch</td>
<td>AVC and University Registrar</td>
<td>1 week</td>
</tr>
<tr>
<td>Internal Assessment, including exam marking</td>
<td>Relevant PVCs</td>
<td>1 week</td>
</tr>
<tr>
<td>Extramural support services and liaison</td>
<td>AVC and University Registrar</td>
<td>1 week</td>
</tr>
<tr>
<td>Industrial relations advisory</td>
<td>AVC – People and Organisational Development</td>
<td>1 week</td>
</tr>
</tbody>
</table>
f) Commitment to maintain and review the University’s Business Continuity Policy, Framework, plans and solutions on a regular basis;
g) Appreciation and recognition of the importance of BCM to the University and the role of individuals within it;
h) Communication to all external stakeholders (and third parties) upon whom the University depends, in both normal and major disruptive events, of the importance of BCM to the University and their roles.

If these approaches are adopted, all those associated with the University should have confidence in its ability to manage the continuity of its operations during an event, and have in place the appropriate behaviour and culture to promote business resilience.

6.2. Outcomes
The outcomes from a BCM cultural development programme should include:

- a clearly defined and documented Business Continuity Policy agreed and signed-off by the University’s executive or senior management (this already exists);
- acceptance and implementation of BCM as a professional management discipline;
- an understanding of the University’s BCM Framework, Policy and supporting plans and management structures;
- an organisational culture that ensures BCM activities and considerations are integral to the business-as-usual activities throughout the University at all levels;
- proactive “hands-on” promotion of BCM by the University’s executive, senior and middle management;
- an organisational, managerial and staff BCM competence to execute the organisation’s BCM strategy;
- an awareness and understanding by the University’s management and staff of the importance of BCM and their roles, accountabilities, responsibilities and authority within it;
- an understanding of the coordination activities that are required between the University’s Emergency Management Teams, departmental Business Continuity Teams and the IT Disaster Recovery Team in the event of a major disruptive event;
- an understanding of which Business Continuity Teams are dependent on one another for performance;
- applicable internal documents and plans as well as external standards and guidelines;
- ongoing BCM education and awareness promotion;
- a performance management and appraisal system (and a rewards and recognition system) that explicitly recognises and reinforces the importance of BCM;
- job descriptions and associated skills that include BCM at specified levels within the organisation;
- an ongoing programme of BCM training for those directly involved in the implementation, maintenance and execution of the University’s BCM capability;
- a clearly defined and documented management information system to monitor and evaluate the BCM awareness and competency of the University’s staff and managers;
7. Training, Testing and Maintenance of Business Continuity Arrangements

As part of the University’s commitment to BCM and an open continuity culture, the University will maintain an active and regular programme of BCM training, testing and review.

7.1. Training

General BCM training, as well as role-specific training, will be provided to all staff.

To improve awareness of the University’s specific BCPs, the following training schedule is to be used:

- Induction training upon appointment for Plan and Function Owners
- Familiarisation training session for Plan Owners and Function Owners annually
- Exercise training for members of University and Campus Emergency Management Teams (refer to the Massey University Strategic Emergency Management Framework for more details).

BCPs and associated personnel are exempt from the training / testing where the following occurs:

- The respective BCP is invoked as part of a real time incident that occurs within the last 12 months;
- An exemption is obtained for the business function that is approved by the responsible AVC/PVC/DVC (for that functional area) 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 Risk Management Office.

7.2. Testing

Plan testing will also be conducted. The University is to implement a progressive testing regime based on meeting performance expectations and seeing improvement in applying basic testing techniques. A three-year testing programme would ideally include:

- In year 1: a desktop test approach for selected Departments. A desktop 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 2: a restricted plan activation and mobilisation activity. Typically, selected critical functions would be required to mobilise resources (e.g. emergency procedures and warden testing) to respond to a presented major disruptive event scenario. This may also involve utilisation of an alternate site.
In year 3: a simulated exercise developed involving multiple functions and potentially impacting an entire site or Campus. The exercise may require re-locating personnel and resources to an alternate site and apply BCPs to respond the major disruptive event scenario.

The outcomes of these reviews and testing activities will be integrated into the existing business structures and processes as well as the BCPs and other emergency response documentation to ensure that the processes remain focused for the University and the plans remain current and reflective of the University's business needs and strategies.

The Risk Management Office will oversee the Testing Programme, keep records of tests, including participation lists and dates.

7.3. Review and Maintenance

7.3.1. Business Continuity Management Framework
The Risk Management Office is responsible for ensuring that a review of this BCM Framework is conducted annually.

7.3.2. Business Impact Analyses (BIAs)
Massey University must:

2. Annually review the Risk Assessment including periodic maintenance of the Business Impact Analysis.

Business Continuity Policy, December 2012

The University-wide BIA and all other BIAs, must be reviewed at least annually.

7.3.3. Business Continuity Plans (BCPs)
Massey University must:

3. Periodically update the Business Continuity Plan (or plans) to ensure currency of information, and response strategies. The plan must be reviewed for possible updating within 30 days of any major operational or system changes that will have a material effect on the contingency strategy of any College/Campus/Section.

Business Continuity Policy, December 2012

BCPs must be reviewed at least annually, in conjunction with the relevant BIA.

BCPs should be updated after each training / testing exercise (if weaknesses or changes are identified) and after actual events, according to outcomes of incident debrief sessions.
Contact names and details within the BCPs (generally contained in the annexes) should be reviewed and updated on a six-monthly basis, or when a restructure occurs (change to operations, change to legislation/compliance, etc), whichever occurs first.

7.3.4. Audit
Internal Audit may review BIAs and BCPs as required by the University’s Internal Audit plan.

8. References
AS/NZS5050:2010 Business Continuity- managing disruption-related risk
ISO31000: Risk Management – principles and guidelines