

Last updated: _____



Business Resilience Handbook



Contents

1. Purpose.....	1
2. Approach.....	1
3. Roles and Responsibilities.....	2
4. Crisis Management Team (CMT).....	3
5. CMT Tasks Flow Chart.....	4
6. CMT Tasks Checklists.....	5
7. Business Continuity Plan.....	10
Appendix 1 : Incident Room Details.....	i
Appendix 2 : Key Contact Details.....	ii
Appendix 3 : Damage Assessment Report.....	iii
Appendix 4 : Stakeholder Communication Plan.....	iv
Appendix 5 : Event Log.....	vi
Appendix 6 : Glossery of Terms.....	viii
Appendix 7 : Evacuation Information.....	x
Appendix 8 : Floor Plan.....	xi

A copy of this handbook is to be retained offsite by each member of the Executive Team, the Crisis Management Team, and a current copy kept in the BCM Box held offsite at the secondary and tertiary incident room locations.

In addition, all members of the Executive Team and the Crisis Management Team will have this handbook and all associated documents stored on two encrypted USB sticks. One USB stick to be kept with laptop, the other in an offsite location such as the home.

Contact your local Ansvar office to speak to a Risk Advisor if you would like help in using this document.

Disclaimer

Ansvar Insurance Limited ("Ansvar") disclaims all responsibility to any party for any loss or liability that any party may suffer or incur arising from or relating to or in any way connected with the contents of this Business Resilience Handbook, or the reliance upon this Business Resilience Handbook by any party. In carrying out our work and preparing this this Business Resilience Handbook, Ansvar has worked solely on the instructions of its management and has not taken into account the interests of any other party. Material events may have occurred since the preparation of this Business Resilience Handbook which is not reflected in this Business Resilience Handbook.

1. Purpose

The purpose of this Business Resilience Handbook is to specify _____ (the “Company”) response to disruptive events that require an organisation-wide response due to the nature of the event and activation of business recovery plans to re-establish time critical processes and recover resources.

2. Approach

This plan is based on a Business Resilience Framework (Figure 1) that describes actions to be taken following a disruptive event and the timeframe to execute these actions.

Timeframes to recover from disruptive events are based on a Minimum Allowable Outage (MAO) for each identified time critical process. There are two ways in which the MAO is met:

- 2.1. WORKAROUNDS – ie an alternative method of restoring the affected process without retrieving the lost or unavailable resources; or
- 2.2. RESOURCE RECOVERY – ie a method used to make the lost or unavailable resources available again.

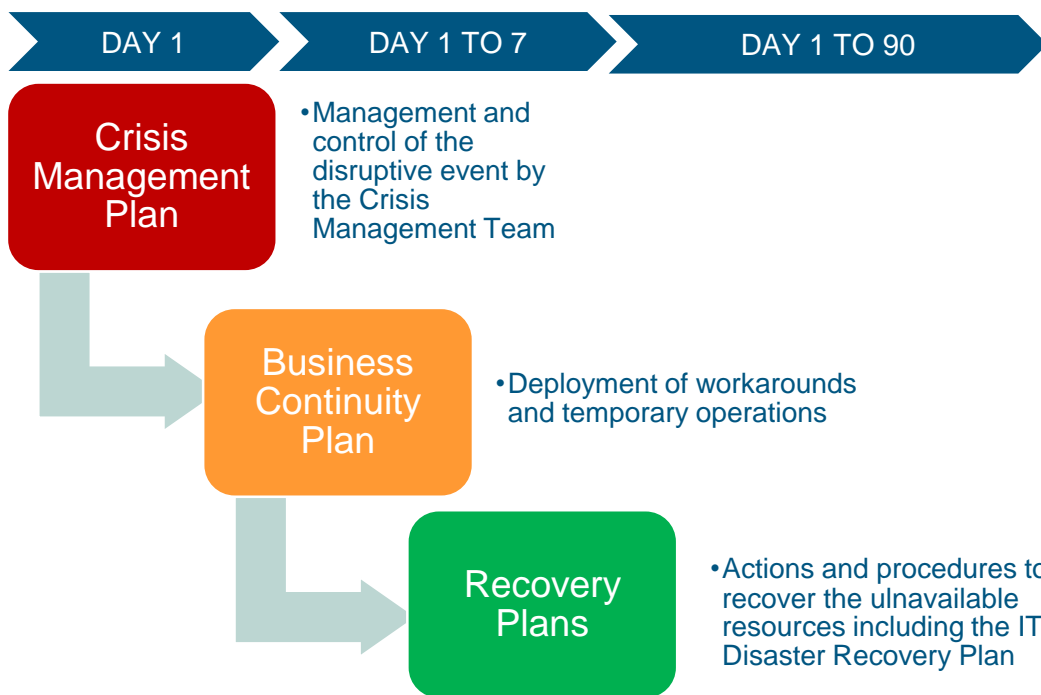


Figure 1: Business Resilience Framework

Colour key for Resilience Plan components



3. Roles and Responsibilities

3.1. Crisis Management Team (CMT)

The CMT coordinates business recovery arising from a disruptive event. The CMT's responsibilities are to ensure the:

- Safety of personnel
- Assessment and containment of damage
- Effective management of people and supplies
- Activating and overseeing the execution of resource recovery plans

3.2. Executive Team

The Executive Team supports the management of the disruptive event through the CMT. This includes assisting and supporting CMT decisions, communicating actions and undertaking any activities as assigned by the CMT. The _____ is accountable for the Business Resilience Plan.

3.3. Resource Providers

Resource providers both internal and external are responsible for the recovery of lost and unavailable resources that they support.

3.4. Process Owners

Process owners are internal staff that oversee or manage key business processes and are responsible for maintaining or restoring the continuity of these disrupted processes. This may be achieved using the deployment of identified workarounds.

3.5. Recovery Plans

Three recovery plans have been developed to restore _____ business services:

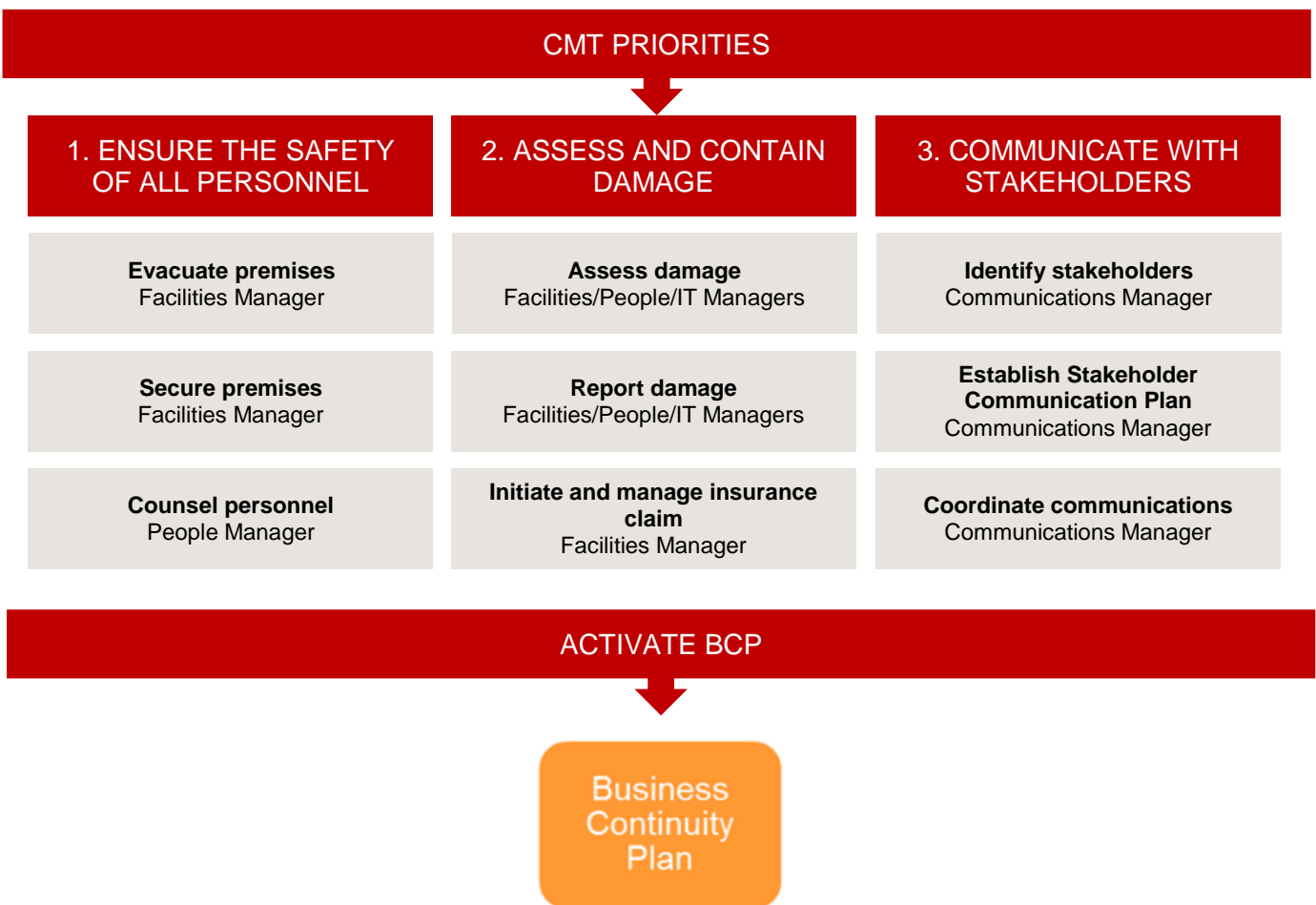
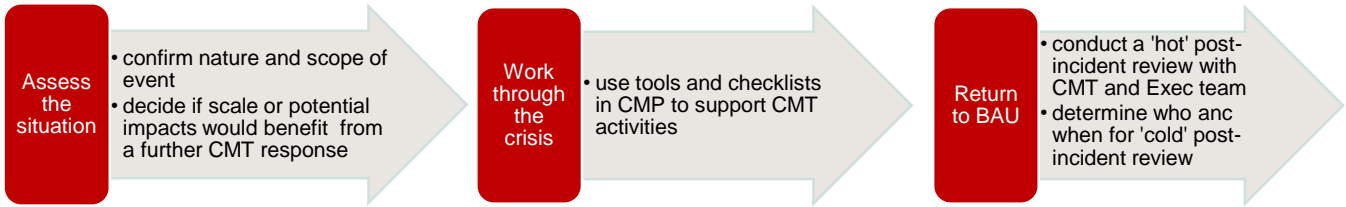
- i. **IT Disaster Recovery Plan** – owned by: _____
- ii. **Facilities Recovery Plan** – owned by: _____
- iii. **People Recovery Plan** – owned by: _____

The recovery plans support both the workarounds for the Business Continuity Plan priority processes and the full recovery of the resources to enable a return to business as usual.

4. Crisis Management Team (CMT)

ROLE	RESPONSIBILITIES	KEY ACTIONS	WHO	
			Primary	Alternative
Crisis Manager	<ul style="list-style-type: none"> Lead CMT Coordinate CMT tasks 	<ul style="list-style-type: none"> Lead CMT Coordinate CMT tasks 		
Crisis Room Manager	<ul style="list-style-type: none"> Prepare and maintain the Crisis Room for use by the CMT Formally log key issues and decisions 	<ul style="list-style-type: none"> Activate and set up room Distribute role cards and task sheets Initiate incident log 		
Communication and Stakeholder Manager	<ul style="list-style-type: none"> Coordinate all internal and external communications and stakeholder management activities during the crisis 	<ul style="list-style-type: none"> Develop and implement a crisis communication plan Develop and implement a stakeholder management plan 		
People Manager	<ul style="list-style-type: none"> Ensure safety of personnel Coordinate workplace requirements 	<ul style="list-style-type: none"> Assess and report impact on people to CMT Communicate HR policy that applies during the disruption Coordinate staff relocations 		
Facilities Manager	<ul style="list-style-type: none"> Address and report on issues relating to facilities 	<ul style="list-style-type: none"> Assess and report impact on premises Recover unavailable facilities 		
Finance Manager	<ul style="list-style-type: none"> Establish and provide financial support to CMT 	<ul style="list-style-type: none"> Initiate expense account for extraordinary expenses for CMT 		
IT Manager	<ul style="list-style-type: none"> Address and report on issues relating to IT 	<ul style="list-style-type: none"> Assess and report impact on IT Recover unavailable IT resources 		
CEO and other non-CMT executives	<ul style="list-style-type: none"> Support and assist decision making of CMT 	<ul style="list-style-type: none"> Contribute to CMT decision making Undertake tasks allocated particularly in relation to execution of communication and stakeholder management plan Be the liaison point for Board members 	All other non-CMT executives	All other non-CMT executives

5. CMT Tasks Flow Chart



6. CMT Tasks Checklists

6.1. CMT Management Checklist

The following checklists detail the tasks that need to be completed to ensure the effective coordination and management of the crisis.

CMT MANAGEMENT CHECKLIST				
INITIAL TASKS		COMMENTS	WHO	DONE
1. Confirm incident	Confirm an event has occurred which may disrupt critical processes		Crisis Mgr	
2. Activate CMT	Call the CMT together to: <ul style="list-style-type: none"> Determine activation of CMT Any other immediate tasks required 		Crisis Mgr	
3. Activate incident room	Activate the Incident Room Refer to Error! Not a valid link.		Crisis Room Mgr	
4. Initiate event log	Initiate the Event Log to record specific issues and events that occur during the management of the event. Refer to Appendix 5 : Event Log		Crisis Room Mgr	
5. Initiate expense account	Initiate the expense account for extraordinary expenses incurred by CMT members and others during the initial management of the crisis		Fin Mgr	
6. Arrange transport, accommodation, meals etc			People Mgr	
ONGOING TASKS		COMMENTS	WHO	DONE
7. Brief CMT	Periodically brief the Crisis Management Team on the situation and progress to date		Crisis Mgr	
8. Collect checklists			Crisis Room Mgr	
CLOSURE TASKS		COMMENTS	WHO	DONE
9. Collect documentation	Collect the following from each Recovery Plan owner: <ul style="list-style-type: none"> All Damage Assessment Reports Event Log 		Crisis Room Mgr	
10. Close and restore incident room	Close and restore incident room to its original state. Collect all documentation etc. and ensure its safe keeping for debriefing.		Crisis Room Mgr	
11. Confirm all processes have been re-established	Validate with each plan owner that all affected processes have recommenced.		Crisis Room Mgr	
12. Set date and location for debriefing	Set a date and location for debriefing session and advise all required attendees.		Crisis Mgr	
13. Stand down CMT			Crisis Mgr	
14. Sign off plan completion	I confirm that all required tasks of the CMT have been completed as necessary.	SIGNATURE: _____	Crisis Mgr	

6.2. Actions - Priority 1. Ensure Safety of Personnel

The following checklist details the tasks that need to be completed in order to ensure the safety of personnel.

ACTIONS - PRIORITY 1. ENSURE SAFETY OF PERSONNEL CHECKLIST				
INITIAL TASKS		COMMENTS	WHO	DONE
1. Evacuate personnel	Confirm with Evacuation Wardens and Chief Warden that Company tenancy floors have been evacuated of all persons and they are accounted for. Refer to Appendix 9 : Evacuation Information.		Facilities Mgr	
2. Treat casualties	Ensure injured persons receive initial treatment (eg first aid) as necessary until emergency services take over. Liaise with Facilities Manager regarding emergency services, etc.		People Mgr	
3. Treat non-injured personnel	Ensure the well-being of non-injured persons (ie mental stress, confusion etc). Decide what to do with staff that are not injured (eg send to another site or send home). Ensure if they are sent home that they are advised how they will know when to return to work and how they will be kept up to date. Provide counselling as required.		People Mgr	
4. Cordon affected area/s	After emergency services clear building / area for staff to return, ensure all areas considered unsafe are cordoned off until made safe.		Facilities Mgr	
ONGOING TASKS		COMMENTS	WHO	DONE
5. Report personnel status	Report the status of personnel to CMT in terms of personnel unaccounted for; and potential unavailability of numbers, skills, etc.		People Mgr	
CLOSURE TASKS		COMMENTS	WHO	DONE
6. Submit checklists	Provide a copy of this completed checklist to the Crisis Room Manager.		People Mgr	

6.3. Actions - Priority 2. Assess and Contain Damage

The following checklist details the tasks that need to be completed in order to ensure the assessment and containment of damage.

ACTIONS – PRIORITY 2. ASSESS AND CONTAIN DAMAGE				
INITIAL TASKS		COMMENTS	WHO	DONE
1. CALL EMERGENCY SERVICES	Ensure an alarm has activated that automatically alerts emergency services to respond to an emergency within the building.		Facilities Mgr	
2. ASSESS PERSONNEL LOSS	Assess the initial casualties / injuries caused to personnel and record these in the Damage Assessment Report (Appendix 3). Submit initial Damage Assessment Report to the Crisis Room Manager and brief as necessary.		People Mgr	
3. ASSESS FACILITY DAMAGE	Assess the initial damage caused to facilities and record these in Damage Assessment Report (Appendix 3). Submit initial Damage Assessment Report to the Crisis Room Manager and brief as necessary.		Facilities Mgr	
4. ASSESS IT DAMAGE	Assess the initial damage caused to information systems and record these in the Damage Assessment Report (Appendix 3). Assess and report available IT assets (eg major business systems, laptops. Wireless cards, interstate office assets etc.). Submit initial Damage Assessment Report to the Crisis Room Manager and brief as necessary.		IT Mgr	
ONGOING TASKS		COMMENTS	WHO	DONE
5. UPDATE PERSONNEL LOG	Continue to assess the casualties / injuries caused to personnel and record these in the Damage Assessment Report (Appendix 3). Submit updated Damage Assessment Report to the Crisis Room Manager and brief as necessary.		People Mgr	
6. UPDATE FACILITY LOSS	Continue to assess the damage caused to facilities and record these in the Damage Assessment Report (Appendix 3). Submit updated Damage Assessment Report to the Crisis Room Manager and brief as necessary.		Facilities Mgr	
7. UPDATE IT LOSS	Continue to assess the damage caused to IT infrastructure and record these in the Damage Assessment Report (Appendix 3). Submit updated Damage Assessment Report to the Crisis Room Manager and brief as necessary.		IT Mgr	
8. LIAISE WITH INSURER	Liaise with the insurer(s) and, based on the updated Damage Assessment Reports, initiate claims where applicable.		Finance Mgr	
CLOSURE TASKS		COMMENTS	WHO	DONE
9. SUBMIT CHECKLISTS	Provide a copy of this completed checklist to the Crisis Room Manager		Facilities Mgr	

6.4. Actions - Priority 3. Communicate with Stakeholders

The following checklist details the tasks that need to be completed in order to ensure the identification and communication management for all stakeholders

ACTIONS - PRIORITY 3. COMMUNICATE WITH STAKEHOLDERS				
INITIAL TASKS		COMMENTS	WHO	DONE
1. IDENTIFY STAKEHOLDERS	Identify all internal and external stakeholders (including media and regulatory bodies) affected or interested in the event that has occurred. Refer to Appendix 4 – Stakeholder Communication and Management Plan.		Comms Mgr	
2. PREPARE STAKEHOLDER COMMUNICATION AND MANAGEMENT PLAN	Prepare a Stakeholder Communication and Management Plan detailing the key stakeholders, communication methods, key messages, and appropriate spokesperson(s) to communicate the messages to the stakeholders(s).		Comms Mgr	
3. EXECUTE STAKEHOLDER COMMUNICATION PLAN	Facilitate the execution of the approved Stakeholder Communication Plan, providing support where required. Refer to Appendix 4 – Stakeholder Communication and Management Plan.		Comms Mgr	
ONGOING TASKS		COMMENTS	WHO	DONE
4. MONITOR STAKEHOLDERS	On an ongoing basis, get feedback from stakeholders and adjust the Stakeholder Communication and Management Plan accordingly.		Comms Mgr	
CLOSURE TASKS		COMMENTS	WHO	DONE
5. SUBMIT CHECKLISTS	Provide a copy of this completed checklist to the Crisis Room Manager.		Comms Mgr	

6.5. Actions - Activate Plans

The following checklist details the tasks that need to be completed in order to activate required BCP and Resource Recovery plans

ACTIONS - ACTIVATE PLANS				
INITIAL TASKS		COMMENTS	WHO	DONE
1. PRIORITISE IMPACTED PROCESSES AND CONTINUITY PLANS	<p>Based on confirmed knowledge of situation and initial Damage Assessment Reports, determine which processes have been affected by this event.</p> <p>Re-prioritise process continuity based on timing and nature of event, and communicate expected process and re-established timing and priorities to all Continuity Plan Owners.</p> <p>Refer to Table 1 – Process Maximum Allowable Outages (MAOs) – for details of all processes and their MAOs and critical times.</p>		Crisis Mgr	
2. ACTIVATE PLANS	<p>Based on the above, activate all necessary Continuity and Recovery Plans by communicating the plan activation to relevant plan owners.</p> <p>Activate subsequent plans as required.</p>		Crisis Mgr	
ONGOING TASKS		COMMENTS	WHO	DONE
3. CONFIRM ACTIVATION	<p>Confirm required plans have been activated and subsequently completed.</p>		Crisis Mgr	
4. TRACK PLAN STATUS	<p>Establish a suitable method to display the status of each plan including the following:</p> <ul style="list-style-type: none"> Revised MAOs Time the plan has been activated % completion of re-establishment of process If the plan has been completed 		Crisis Mgr	
5. TREAT NON-CRITICAL PROCESSES	<p>If the incident is likely to result in prolonged interruption to the business, consider the continuity of non-time critical functions.</p>		Crisis Mgr	
CLOSURE TASKS		COMMENTS	WHO	DONE
6. SUBMIT CHECKLISTS	<p>Provide a copy of this completed checklist to the Crisis Room Manager.</p>		Crisis Mgr	

7. Business Continuity Plan

The workarounds described in this section are to be deployed following approval by the Crisis Management Team, and are based on the Business Impact Analysis conducted on _____.

The workarounds cover the _____ time-critical business processes, being:

TIME CRITICAL BUSINESS PROCESSES	WORKAROUND IN PLACE
1.	Within ____ hours
2.	Within ____ hours
3.	Within ____ hours
4.	Within ____ hours
5.	Within ____ hours
6.	Within ____ hours
7.	Within ____ hours
8.	Within ____ hours
9.	Within ____ hours
10.	Within ____ hours

7.1. Critical Process 1 – _____

This process is supported by the following business units, and must be re-established within ____ hours:

Business Unit: _____
Business Unit: _____

Business Unit: _____
Business Unit: _____

7.1.1. Employees

In order to re-establish the above process, the Company would require the following minimum number of employees, with the require skills accommodated as per the stated workarounds. (Insert additional rows if required)

FUNCTION	NO. OF EMPLOYEES REQUIRED	SKILLS / KNOWLEDGE REQUIRED	WORKAROUNDS (a brief explanation of the alternative process or workaround to be deployed)

7.1.2. IT Systems

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable IT systems are recovered. (Insert additional rows if required)

IT SYSTEM	WORKAROUND	NO. OF DAYS WORKAROUND CAN BE SUSTAINED FOR

7.1.3. Suppliers

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable suppliers are recovered. (Insert additional rows if required)

SUPPLIER	WORKAROUND	NO. OF DAYS WORKAROUNDS CAN BE SUSTAINED FOR

7.2. Critical Process 2 – _____

This process is supported by the following business units, and must be re-established within ____ hours:

Business Unit: _____
Business Unit: _____

Business Unit: _____
Business Unit: _____

7.2.1. Employees

In order to re-establish the above process, the Company would require the following minimum number of employees, with the require skills accommodated as per the stated workarounds. (Insert additional rows if required)

FUNCTION	NO. OF EMPLOYEES REQUIRED	SKILLS / KNOWLEDGE REQUIRED	WORKAROUNDS (a brief explanation of the alternative process or workaround to be deployed)

7.2.2. IT Systems

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable IT systems are recovered. (Insert additional rows if required)

IT SYSTEM	WORKAROUND	NO. OF DAYS WORKAROUND CAN BE SUSTAINED FOR

7.2.3. Suppliers

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable suppliers are recovered. (Insert additional rows if required)

SUPPLIER	WORKAROUND	NO. OF DAYS WORKAROUNDS CAN BE SUSTAINED FOR

7.3. Critical Process 3 – _____

This process is supported by the following business units, and must be re-established within ____ hours:

Business Unit: _____
Business Unit: _____

Business Unit: _____
Business Unit: _____

7.3.1. Employees

In order to re-establish the above process, the Company would require the following minimum number of employees, with the require skills accommodated as per the stated workarounds. (Insert additional rows if required)

FUNCTION	NO. OF EMPLOYEES REQUIRED	SKILLS / KNOWLEDGE REQUIRED	WORKAROUNDS (a brief explanation of the alternative process or workaround to be deployed)

7.3.2. IT Systems

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable IT systems are recovered. (Insert additional rows if required)

IT SYSTEM	WORKAROUND	NO. OF DAYS WORKAROUND CAN BE SUSTAINED FOR

7.3.3. Suppliers

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable suppliers are recovered. (Insert additional rows if required)

SUPPLIER	WORKAROUND	NO. OF DAYS WORKAROUNDS CAN BE SUSTAINED FOR

7.4. Critical Process 4 – _____

This process is supported by the following business units, and must be re-established within ____ hours:

Business Unit: _____
Business Unit: _____

Business Unit: _____
Business Unit: _____

7.4.1. Employees

In order to re-establish the above process, the Company would require the following minimum number of employees, with the require skills accommodated as per the stated workarounds. (Insert additional rows if required)

FUNCTION	NO. OF EMPLOYEES REQUIRED	SKILLS / KNOWLEDGE REQUIRED	WORKAROUNDS (a brief explanation of the alternative process or workaround to be deployed)

7.4.2. IT Systems

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable IT systems are recovered. (Insert additional rows if required)

IT SYSTEM	WORKAROUND	NO. OF DAYS WORKAROUND CAN BE SUSTAINED FOR

7.4.3. Suppliers

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable suppliers are recovered. (Insert additional rows if required)

SUPPLIER	WORKAROUND	NO. OF DAYS WORKAROUNDS CAN BE SUSTAINED FOR

7.5. Critical Process 5 – _____

This process is supported by the following business units, and must be re-established within ____ hours:

Business Unit: _____
Business Unit: _____

Business Unit: _____
Business Unit: _____

7.5.1. Employees

In order to re-establish the above process, the Company would require the following minimum number of employees, with the require skills accommodated as per the stated workarounds. (Insert additional rows if required)

FUNCTION	NO. OF EMPLOYEES REQUIRED	SKILLS / KNOWLEDGE REQUIRED	WORKAROUNDS (a brief explanation of the alternative process or workaround to be deployed)

7.5.2. IT Systems

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable IT systems are recovered. (Insert additional rows if required)

IT SYSTEM	WORKAROUND	NO. OF DAYS WORKAROUND CAN BE SUSTAINED FOR

7.5.3. Suppliers

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable suppliers are recovered. (Insert additional rows if required)

SUPPLIER	WORKAROUND	NO. OF DAYS WORKAROUNDS CAN BE SUSTAINED FOR

7.6. Critical Process 6 – _____

This process is supported by the following business units, and must be re-established within ____ hours:

Business Unit: _____
Business Unit: _____

Business Unit: _____
Business Unit: _____

7.6.1. Employees

In order to re-establish the above process, the Company would require the following minimum number of employees, with the require skills accommodated as per the stated workarounds. (Insert additional rows if required)

FUNCTION	NO. OF EMPLOYEES REQUIRED	SKILLS / KNOWLEDGE REQUIRED	WORKAROUNDS (a brief explanation of the alternative process or workaround to be deployed)

7.6.2. IT Systems

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable IT systems are recovered. (Insert additional rows if required)

IT SYSTEM	WORKAROUND	NO. OF DAYS WORKAROUND CAN BE SUSTAINED FOR

7.6.3. Suppliers

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable suppliers are recovered. (Insert additional rows if required)

SUPPLIER	WORKAROUND	NO. OF DAYS WORKAROUNDS CAN BE SUSTAINED FOR

7.7. Critical Process 7 – _____

This process is supported by the following business units, and must be re-established within ____ hours:

Business Unit: _____
Business Unit: _____

Business Unit: _____
Business Unit: _____

7.7.1. Employees

In order to re-establish the above process, the Company would require the following minimum number of employees, with the require skills accommodated as per the stated workarounds. (Insert additional rows if required)

FUNCTION	NO. OF EMPLOYEES REQUIRED	SKILLS / KNOWLEDGE REQUIRED	WORKAROUNDS (a brief explanation of the alternative process or workaround to be deployed)

7.7.2. IT Systems

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable IT systems are recovered. (Insert additional rows if required)

IT SYSTEM	WORKAROUND	NO. OF DAYS WORKAROUND CAN BE SUSTAINED FOR

7.7.3. Suppliers

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable suppliers are recovered. (Insert additional rows if required)

SUPPLIER	WORKAROUND	NO. OF DAYS WORKAROUNDS CAN BE SUSTAINED FOR

7.8. Critical Process 8 – _____

This process is supported by the following business units, and must be re-established within ____ hours:

Business Unit: _____
Business Unit: _____

Business Unit: _____
Business Unit: _____

7.8.1. Employees

In order to re-establish the above process, the Company would require the following minimum number of employees, with the require skills accommodated as per the stated workarounds. (Insert additional rows if required)

FUNCTION	NO. OF EMPLOYEES REQUIRED	SKILLS / KNOWLEDGE REQUIRED	WORKAROUNDS (a brief explanation of the alternative process or workaround to be deployed)

7.8.2. IT Systems

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable IT systems are recovered. (Insert additional rows if required)

IT SYSTEM	WORKAROUND	NO. OF DAYS WORKAROUND CAN BE SUSTAINED FOR

7.8.3. Suppliers

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable suppliers are recovered. (Insert additional rows if required)

SUPPLIER	WORKAROUND	NO. OF DAYS WORKAROUNDS CAN BE SUSTAINED FOR

7.9. Critical Process 9 – _____

This process is supported by the following business units, and must be re-established within ____ hours:

Business Unit: _____
Business Unit: _____

Business Unit: _____
Business Unit: _____

7.9.1. Employees

In order to re-establish the above process, the Company would require the following minimum number of employees, with the require skills accommodated as per the stated workarounds. (Insert additional rows if required)

FUNCTION	NO. OF EMPLOYEES REQUIRED	SKILLS / KNOWLEDGE REQUIRED	WORKAROUNDS (a brief explanation of the alternative process or workaround to be deployed)

7.9.2. IT Systems

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable IT systems are recovered. (Insert additional rows if required)

IT SYSTEM	WORKAROUND	NO. OF DAYS WORKAROUND CAN BE SUSTAINED FOR

7.9.3. Suppliers

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable suppliers are recovered. (Insert additional rows if required)

SUPPLIER	WORKAROUND	NO. OF DAYS WORKAROUNDS CAN BE SUSTAINED FOR

7.10. Critical Process 10 – _____

This process is supported by the following business units, and must be re-established within ____ hours:

Business Unit: _____
Business Unit: _____

Business Unit: _____
Business Unit: _____

1.1.1. Employees

In order to re-establish the above process, the Company would require the following minimum number of employees, with the require skills accommodated as per the stated workarounds. (Insert additional rows if required)

FUNCTION	NO. OF EMPLOYEES REQUIRED	SKILLS / KNOWLEDGE REQUIRED	WORKAROUNDS (a brief explanation of the alternative process or workaround to be deployed)

1.1.2. IT Systems

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable IT systems are recovered. (Insert additional rows if required)

IT SYSTEM	WORKAROUND	NO. OF DAYS WORKAROUND CAN BE SUSTAINED FOR

1.1.3. Suppliers

In order to re-establish the above process, the Company would require the deployment of the stated workarounds until unavailable suppliers are recovered. (Insert additional rows if required)

SUPPLIER	WORKAROUND	NO. OF DAYS WORKAROUNDS CAN BE SUSTAINED FOR

Appendix 1 : Incident Room Details

INCIDENT ROOMS

Primary Location

Secondary Location

Tertiary Location

Appendix 2 : Key Contact Details

	<i>Primary</i>		<i>Alternative</i>	
Crisis Manager				
Crisis Room Manager				
Communication and Stakeholder Manager				
People Manager				
Facilities Manager				
Finance Manager				
IT Manager				
Other non-CMT executives				

Appendix 3 : Damage Assessment Report

DATE AND TIME	AFFECTED RESOURCE	DAMAGE ASSESSMENT	MADE BY	WHAT ACTION WAS TAKEN

Appendix 4 : Stakeholder Communication Plan

CATEGORY	STAKEHOLDER NAME	STAKEHOLDER CONTACT	COMUNICATION METHOD	KEY MESSAGES	SPOKESPERSON
Customers					
Brokers					
Board & Group					
Emergency Services - Police - Fire & Rescue					

CATEGORY	STAKEHOLDER NAME	STAKEHOLDER CONTACT	COMMUNICATION METHOD	KEY MESSAGES	SPOKESPERSON
Employees / Families					
Regulators					
Suppliers					
Other					

Appendix 5 : Event Log

TIME AND DATE	EVENT DESCRIPTION	ACTION TAKEN

TIME AND DATE	EVENT DESCRIPTION	ACTION TAKEN

Appendix 6 : Glossery of Terms

Business Continuity Plan (BCP) – documented procedures that guide the organisation to respond, recover, resume and restore to a predefined level of operation following a disruption.

Business Resilience Framework (BRF) – comprises the following components: Crisis Management Plan, Business Continuity Plan and Recovery Plans. These documents are supported by the underlying business impact analysis.

Business Impact Analysis (BIA) – a process to identify or verify how long the Company can delay the performance of key processes (known as the Maximum Allowable Outage). The outcome of the business impact analysis is the identification of the Company's mission critical processes.

Cold (Formal) Debrief – a discussion held within weeks of an exercise or incident addressing the wider organisational issues that identifies learning opportunities.

Crisis Management Plan – a set of processes, actions and tools that assists the designated Crisis Management Team to manage and control a disruptive event.

Crisis Management Team (CMT) – key senior staff and process specialists whose role it is to manage and control a disruption event.

Disruption Event – an event that causes the loss or unavailability of one or more critical resources, such as the Company's premises. A crisis event impairs the Company's ability to perform business as usual processes (BAU), and requires the crisis management and business continuity plans to be invoked. Eg a gas leak that prevents staff from accessing/using the Company's Head Office building, or a widespread power outage in the vicinity of the Company's Head Office.

Facilities Disaster Recovery Plan – detailed procedure documents that specify how to restore facilities resources.

Hot (Formal) Debrief – a discussion about the issues and concerns held immediately following the decommissioning of the CMT after an incident.

IT Disaster Recovery Plan – detailed procedure documents that specify how to restore IT systems.

Maximum Allowable Outage (MAO) – the maximum time acceptable before the service or activity must be resumed through either a workaround or through recovering the unavailable resource.

Mission Critical Processes – critical time sensitive business processes the Company must perform within the agreed maximum allowable outages.

People Disaster Recovery Plan – detailed procedure documents that specify how to restore people resources.


Recovery Plans – detailed procedure documents that specify how to recover key resources such as IT, People, Facilities and Suppliers.


Recovery Point Objectives (RPO) – relates only to IT systems and indicates how much data could be lost from the system without too much impact considering that the data may need to be re-entered later and there may be work back-log clearing. The RPO is used by IT to design suitable backup regimes. For example, an RPO of 1 day, means IT only needs to have backups for that data once a day (typically overnight). In this case up to 1 day's worth of data could be lost from systems I, say, the system is destroyed just after backup is made and taken offsite.


Recovery Time Objective (RTO) – the time at which the resources must be recovered if it were to become unavailable. The RTO is calculated by the shortest MAO for processes needing the resources PLUS the PERIOD (ie the duration a related workaround could be practically sustained). It means that the resources would be made available again, at the time the workaround could not be sustained any longer.

Workarounds – activities and processes that enable the business units to perform the identified mission critical processes within the maximum allowable outage period, whilst access to BAU resources such as IT and buildings are being recovered. For example, working offsite with remote access, manual payment processing

Appendix 7 : Evacuation Information

Fire Wardens				
	Location	Warden	Contact Details	

First Aid Officers				
	Location	Warden	Contact Details	

Health & Safety Committee Members				
	Location	Warden	Contact Details	

Appendix 8 : Floor Plan