15. How to Develop a Business Continuity Plan

PURPOSE & CRITERIA

The WQA Standard sets out the requirements of vendors to reduce the probability of a crisis occurring and respond to and recover from a crisis. This requirement is intended to ensure vendors have taken all possible and realistic steps to ensure the continuity of supply to Woolworths in the event of a major interruption impacting the vendor's operations.
This "how to" guide should be read in conjunction with the WQA requirements. The guide provides basic information as to how you can assess your business and develop an appropriate Crisis / Business Continuity Plan. There is no requirement for businesses to use this guide. It is offered as a means of assistance for those organisations who may like some general advice or guidance to meet this particular element of the standard.

The guide has been simplified from the full Business Continuity Process and does not take into account individual businesses circumstances (e.g. size, complexity etc). Every business or organisation should consider its own situation and requirements when using these guidelines.

DEFINITIONS

Business Continuity (BC): the "uninterrupted availability of all key resources supporting essential business functions".

Business Interruption: an event whether anticipated (e.g. a strike) or unanticipated (e.g. power outage, flood) which disrupts the normal course of business operations at an organisation location.

Business Impact Analysis (BIA): used to identify and measure the effect of resource loss and escalating resource loss over a period of time in order to base decisions on risk mitigation and continuity planning.

Business Continuity Plan (BCP): a collection of procedures and information which is developed, compiled and maintained in readiness for use in the event of a significant business interruption which may not be able to be handled using business as usual management strategies.

Likelihood: the probability or frequency of an event occurring.

Impact: is the outcome following the occurrence of an event.

Hazard / Risk: A potential source of harm. This could be the origin or nature of the expected harm.

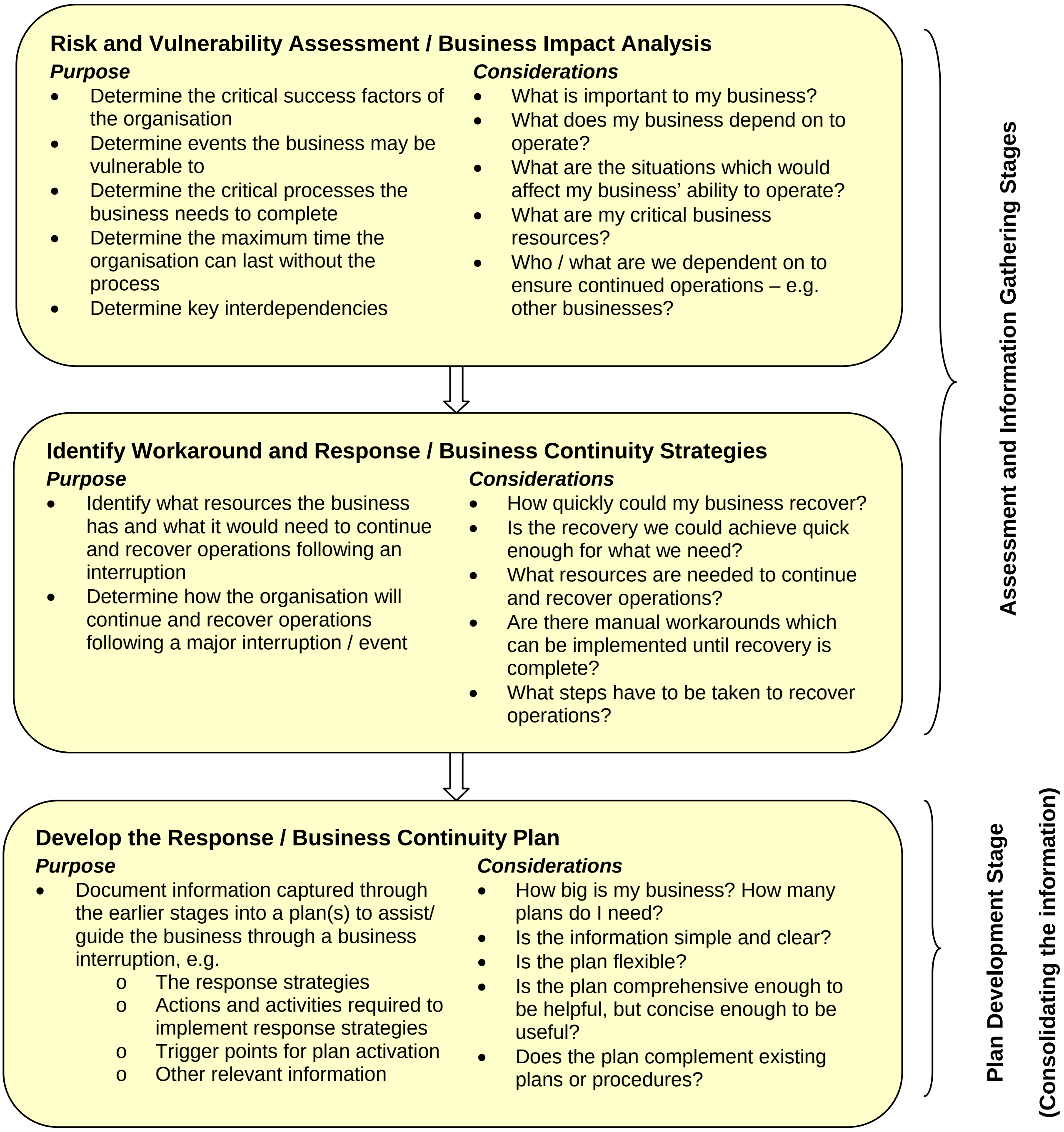
Maximum Tolerable Outage (MTO): The maximum period of time a critical business process can operate before the loss of process affects operations to an irreparable level.

Recovery Time Objective (RTO): The period of time which is actually required to fully re-establish adequate resource requirements.

Recovery Strategy: A pre-defined, pre-tested course of action to be undertaken in response to a business interruption or disaster.

DEVELOPING A RESPONSE / BUSINESS CONTINUITY PLAN

The following is a simplified version of the Business Continuity Plan (BCP) development process. The stages below are explained in detail throughout the next sections.



Risk and Vulnerability Assessment / Business Impact Analysis

Purpose

- Determine the critical success factors of the organisation
- Determine events the business may be vulnerable to
- Determine the critical processes the business needs to complete
- Determine the maximum time the organisation can last without the process
- Determine key interdependencies

Considerations

- What is important to my business?
- What does my business depend on to operate?
- What are the situations which would affect my business' ability to operate?
- What are my critical business resources?
- Who / what are we dependent on to ensure continued operations – e.g. other businesses?

Identify Workaround and Response / Business Continuity Strategies

Purpose

- Identify what resources the business has and what it would need to continue and recover operations following an interruption
- Determine how the organisation will continue and recover operations following a major interruption / event

Considerations

- How quickly could my business recover?
- Is the recovery we could achieve quick enough for what we need?
- What resources are needed to continue and recover operations?
- Are there manual workarounds which can be implemented until recovery is complete?
- What steps have to be taken to recover operations?

Assessment and Information Gathering Stages

Develop the Response / Business Continuity Plan

Purpose

- Document information captured through the earlier stages into a plan(s) to assist/ guide the business through a business interruption, e.g.
    - The response strategies
    - Actions and activities required to implement response strategies
    - Trigger points for plan activation
    - Other relevant information

Considerations

- How big is my business? How many plans do I need?
- Is the information simple and clear?
- Is the plan flexible?
- Is the plan comprehensive enough to be helpful, but concise enough to be useful?
- Does the plan complement existing plans or procedures?

Plan Development Stage

(Consolidating the information)

STAGE ONE: Risk and Vulnerability Assessment / Business Impact Analysis

Note: *Throughout this section, examples of templates are provided to help illustrate how and what information can be collected. These templates are included in the Appendix of this document.*

The Risk and Vulnerability Assessment/Business Impact Analysis is designed to capture the relevant and important information which will assist the business identify what needs to be considered for inclusion into any Response/Continuity Plan.

a) Understanding the Business and Its Vulnerabilities

The core processes are the activities which form the heart of what the business unit does, its primary functions, or its reason to exist.

Once identified, the core processes become the focus of discussion for completing the BIA and recovery strategy. For the purpose of completing the BIA, the processes should be kept at a reasonably high level. Between 3 to 10 processes is a good number.

Maximum Tolerable Outage defines the disruption or down-time tolerance threshold for the core process i.e. how long the business can be without this process before it suffers unacceptable loss/damage. The MTO is then used to determine the time period in which the process must be resumed **/** recovered.

As a guide, the following timeframes can be used:

12 hours; 24 hours; 48 hours; 72 hours; 1 week; 2 weeks, 4 weeks & >4 weeks. Not Applicable (NA) can be used when the process is low priority and not time dependent.

In circumstances where the scenario could cause an increasing degradation of resources / capability over a period of time, you should select the **worst** case option. This may need to be based on past previous experience or expected.

The likelihood assessment is a rough estimation of the chance of each business interruption event occurring. When assessing this, assume there are no controls in place to mitigate this event occurring.

Refer to ***Table 2*** for example of likelihoods.

Business Impact Analysis						
Process Name & Summary Description	**Worst Case Risk Event / Threat for Process**	**Maximum Tolerable Outage**	**Recovery Time Objective**	**Likelihood**	**Impact**	**Overall Risk Rating**
Despatch	Loss of IT Systems	48 hours	72 hours	Possible	Medium	Medium

The worst case risk event / threat should be used to highlight the worst type of event which could impact the particular core process. **Together, these risk / events help identify what types of response plans / recovery strategies your BC Plan should contain.**
To reduce complexity of any Plan it can be useful to use threat / hazard categories, rather than individual threats. Refer to ***Table 1*** for examples.

The Recovery Time Objective is the time it will actually take to recover the process following the event (choose worst case timeframe)

Where there is a gap between the MTO and RTO, workarounds need to be investigated

The impact assessment is calculated in either **financial or non-financial** terms. It considers what impact (consequence) the business interruption event would have on the core process.

You should determine what the impact would be if the core process could not be continued assuming there are no contingencies in place to mitigate the risk exposure (e.g. Plans).

Refer to ***Table 3***

The overall level of risk or *risk rating* is determined through combining the consequence and likelihood estimations.

Refer to ***Table 4***

This allows you to determine where best to focus or prioritise your attention in a BC event and confirms what has a high enough risk rating to need to go into a Plan.

Table 1 – Examples of threats and hazards

Threat / hazard category	Potential threat or hazard
Property and other damage	Structural damage Loss of building / facility / asset Fire Explosion Hazardous Material incident Radiological exposure Vandalism Flood Poor maintenance Wear and tear
Natural Events	Flood Drought Earthquake Bushfire Storm (thunder / snow etc) Cyclone Pandemic Ash Cloud Severe Cold / Heat
Human Behaviour	Terrorism Fraud Theft Misappropriation Bomb / Bomb threat Civil disturbance or riot Extortion Kidnap / abduction Armed hold up Siege Human error Sabotage Mass Casualty incident VIP situation Civil disturbance Industrial action
Technology & Technical Issues	IT systems failure (hardware / software) Loss of key utility (power, water, gas) Hazmat exposure Supply shortage Transportation failure A/C or heating failure
Commercial and Legal Relationships	Litigation Strike Product contamination Contractual clauses Supply chain Insurance claim
Political Circumstances	Government Policy / direction Government instability Changes in legislation / regulation Regulator involvement
Occupational Health and Safety	Fatality on site Serious Injury on site Contamination of site or air supply e.g. Anthrax threat etc

Table 2 – Examples of Likelihood Criteria

Determining Likelihood	
Likelihood	**Criteria**
Almost Certain	Will occur repeatedly within the budget period unless action taken
Likely	On balance of probability will occur, or Could occur within 'months to years'
Possible	May occur shortly but a distinct probability it won't, or Could occur within "one to five" years
Unlikely	May occur, but not anticipated, or Could occur in "five to ten" years
Rare	Occurrence requires exceptional circumstances Exceptionally unlikely, even in the long term future Less than a "once in ten year" event

Table 3 - Examples of Impacts – Financial and Non Financial

Examples of disruption impacts on the organisation	
Class of Impact	**Areas of Impact**
Financial impacts	Opportunity cost Increased trading / operating costs Losses of revenue Losses due to physical damage or injuries Capital value Increased expenses during recovery period
Non-financial impacts	Corporate reputation, brand or adverse publicity Delivery standards Legal, contractual or regulatory liabilities Intellectual property, knowledge and data Stakeholder confidence and goodwill Staff morale and well being Loss of management control

Examples of financial impacts	
Category	**Description**
Very Low	Financial loss <1% EBIT or operating budget equivalent
Low	Financial loss >1% EBIT or operating budget equivalent
Medium	Financial loss >3% EBIT or operating budget equivalent
High	Financial loss >5% EBIT or operating budget equivalent
Very High	Financial loss >10% EBIT or operating budget equivalent

Examples of non-financial impacts	
Category	**Description**
Very Low	No measurable operational impact to the business
Low	Minor degradation of service, impact limited to a single area of the business, local management intervention required
Medium	Substantial degradation of service, impact to multiple areas of the business, substantial management intervention required
High	Significant degradation of operations or service delivery, impact to multiple and diverse areas of the business, significant senior management intervention required and possible external assistance
Very High	Widespread and total degradation of operations or service delivery, impact across critical functions of the organisation threatening the immediate or ongoing viability of the organisation, immediate senior executive and / or Board intervention required.

Table 4- Risk Rating Matrix

Likelihood Rating		Impact / Consequence Rating				
		Very Low	Low	Medium	High	Very High
	Almost Certain	Medium	High	Very High	Very High	Very High
	Likely	Medium	Medium	High	Very High	Very High
	Possible	Low	Medium	Medium	High	Very High
	Unlikely	Low	Low	Medium	Medium	High
	Rare	Low	Low	Low	Medium	Medium

b) *Determining Resource Requirements*

For each critical business function, identify the minimum resources which would be needed to maintain continuity of operations whilst a recovery is underway. This may be in an alternate workplace using alternate / reduced resources.

Identify the specific critical business function

Minimum Resource Requirements								
Critical Business Function / Process	Despatch							
Resources	Resource Requirements *Minimum levels required to complete key business process*						Normal Resource Level	Manual Workarounds (Yes / No)
	Day 1	Day 2	Day 3	1 Week	2 Weeks	Over 2 weeks		
Staff	0 0	1 2	1 5	1 8	1 10	1 10	1 Manager 10 staff	NA
PC's	0	0	2	3	4	4	4	Yes

Identify each type of resource required eg staff, telephones, desks, computers

Identify minimum resourcing requirements for each time period following the disruption event

Record current or normal resourcing levels

Determine if manual workarounds or other alternate solutions are available

c) Identifying Key Business Dependencies

Interdependencies could impact the continuity of operations or the recovery of operations should be captured. This may be between critical business functions within your business, or with key suppliers, customers, partners etc. E.g. – What would happen if a key supplier you rely upon was unable to provide the service you need from them.

List the companies or businesses your business relies on to continue its core processes

What are the options to continue critical process in absence of dependent parties good / service?

Key Business Dependencies

Name of Key Party	Supports Critical Process	Tolerable Outage Time	Impact Summary	Continuity Strategy / Workaround
Bob's Boxes	Packaging	48 hours	Unable to package products resulting in backlog in production and delays in delivery to customer..	Utilise reserve packing SOH. Contact Chris' Cartons for product.

Which of your businesses critical processes does this party support?

How long can your business last without this party?

What would happen if the dependent parties' goods or services are unavailable longer than your tolerable outage time?

STAGE TWO: Identify Workaround and Response / Business Continuity Strategies

The development of workarounds and response strategies is concerned with determining how the business will respond, function to an acceptable capability and then recover operations following a major interruption event.

a) Determining Alternate Workarounds

Where the recovery timeframe exceeds the maximum tolerable outage, and core processes cannot be maintained, alternate workarounds may need to be implemented. Commonly, manual processes are used to replace the non-available automated process, e.g. a simple alternate workaround for a word processor may be the use of pen and paper.

Manual workarounds can be used as part of the overall response strategy to keep the business functioning to some capacity until recovery has been completed.

Record the core process / business function identified previously

Alternate Workarounds			
Critical Business Function / Process		Despatch	
Critical resource requirement	**What critical tasks / activities / processes can be performed?**	**What critical tasks / activities / processes cannot be performed?**	**What alternative processes or workarounds can be employed?**
"Daily Deliverer" Software & Database	Preparation of packages for despatch	• Auto labelling and despatch of products • Auto uploads of delivery data to courier companies • Auto progress updates to customers of delivery status	• Revert to excel customer database for address details • Ring / fax courier companies to arrange pick up and deliveries • Ring customers and advise of progress of delivery/ have courier company advise customer of delivery status

Populate with critical resource requirements (as identified in minimum resource requirement section)

Identify what can still proceed in the total absence of the required infrastructure

Identify what cannot proceed in the total absence of the required infrastructure

Identify any viable workarounds which can be used.

b) *Develop Response / Business Continuity Strategies*

The development of Response / Business Continuity strategies is concerned with determining how an organisation will react to an incident. In the development of any strategies, there are a number of issues which must be considered e.g.:

a) Regulatory, policy or industry standard requirements must be addressed
b) Cost and benefit of strategy options
c) Additional risks created by the strategy options
d) Capability to implement the strategies

Strategies may be required for the following stages:

a) Emergency Response – Immediate reaction to a disruption focusing on the protection and preservation of property (These may already be in existence – e.g. evacuation procedures etc)
b) Continuity Phase – Focusing on establishing a minimum acceptable level of capability and performance
c) Recovery Phase - Focusing on returning to routine / long term operational capacity and performance.

Strategy Development Template			
Critical Business Process / Function	Despatch		
Critical Infrastructure	"Daily Deliverer" software & database		
Risk Scenario	Loss of IT Systems		
MTO Time	24 hours	**RTO time**	72 hours
Response Requirements	Establish alternate despatch procedure and capability to cover 48 hour gap period before recovery can be achieved by Business Technology Services		
Response Option 1	Purchase second IT server and house a back up copy of Daily Deliverer software on it	CBA	Not favourable
Response Option 2	Revert to manual procedures to prioritise, label and deliver product	CBA	Favourable
Response Option 3		CBA	
Response Option 4		CBA	
Recommended Option	Revert to manual procedures to prioritise, label and deliver product	**Response Objectives**	Resume despatch capability to 50% within 24 hours
Detailed Description of Response	• Contact production and packaging and advise of systems failure and delays may occur with despatch. Managers to consider altering production schedule. • Contact courier companies and advise automated link is down, and will be reverting to fax / phone. • Revert to excel database for customer and order details. Print delivery dockets manually using dot matrix printer. • Reconcile deliveries to Daily Deliverer when restored		
Preparatory Requirements		**Responsibility**	
	• Develop list of customers and courier companies on excel file	• Fred Smith	
	• Develop a list of delivery schedules on excel file	• John Doe	
	• Establish file on excel for merging of delivery schedules with customer details	• Steve Idore	
	• Arrange for reserve stock of manual delivery dockets to be kept in despatch office	• Mark Cando	

Develop options to address the response requirements

Undertake a cost benefit analysis for each option

Describe key components of recommended response option

Identify actions which have to be completed before plans are completed

Identify responsible people for each preparatory action

STAGE THREE: Develop the Response / Business Continuity Plan

The information gathered in the previous sections, can now be used to identify and prioritise what needs to be contained in any response or continuity plan(s).
For example, you will now know:

- what risk events the business is vulnerable to
- what the core processes are which are most valuable or vulnerable to an interruption
- how long you have to recover the processes before the business is significantly impacted following a specific interruption
- how vulnerable you are to the loss of a key supplier

- what you can do to work around the loss of a core process until it is restored
- how you will go about recovering the process and your operations

The structure and content of a Plan will depend upon the context of each individual organisation. A small business may only require one plan to be developed to meet all its requirements, whereas a medium to large business may require multiple plans to be developed – one for each of its critical business functions and / or key locations. Alternately, you may do a plan for each key risk event which was identified – e.g. natural events, technology and technical issues etc.

As a result of this, a plan template has not been included with this guide.
Below is a general guide as to how a plan can be written and what can be included in it.

a) Basic Principles

The plan should be written so it can be understood by those expected to use it. Any plan should also be able to be used by someone during an event that has not previously seen the document.
The key issues to consider when writing the plan include the following:

Simplicity	Use easy to understand and follow steps
Language	Avoid using acronyms and slang. Write for the average person, not the technical specialist
Assumptions	Don't assume the reader will know the key requirements. If it's important – document it
Clarity	Provide information in a format which can be readily understood. Test its readability with people not familiar with the area covered by the plan
Flexibility	The plan may be required in response to one of many different scenarios. Avoid writing for an isolated or limiting scenario
Comprehensive	Provide sufficient detail to make it a useable document which will inform and direct actions following a major disruption event
Brevity	Avoid creating lengthy volumes or plans which are too wordy to be easily followed when activated
Achievable	The requirements detailed in the plan must be achievable in the circumstances which are likely to be occurring when the plan is activated
Complementary	Plans must compliment other plans. Different plans should not promote competition for scarce resources
Confidentiality	Plans need to be accessed by a number of individuals. Appropriate privacy controls need to be implemented
Accessibility	Plans need to be readily accessible. Copies of the plan may need to be held in several locations to ensure it can be accessed at any time and in any situation

b) Plan Content

As a minimum the following generic information should be included:

- Version control
- Criteria for Plan activation
- Specific actions and responsibilities

- Resource requirements
- Communication requirements
- Contact lists

Further to above, the following section provides more detailed information as to what you may want to include in your Plan.

i) Small to Medium Organisation

Front Page	• Name of business / organisation • Name of business unit / group / team • Name of Business Continuity Plan • Version Number • Month / Year of Plan
Body of Plan	• Review and distribution lists • Plan authorisation • Purpose of plan • Assumptions or limitations of plan • Related documents • Plan activation o overview of when the plan will be activated and implemented o escalation triggers o identify detailed checklists in Appendices • Location of alternate facilities & / or accommodation (if required) • Resource requirements
Appendix	• Emergency response checklist • Continuity checklist • Recovery checklist } What has to happen / who will do it / when it will be done • Systems / specific items details • Contact details o internal o external

ii) Large Organisation

	Content	**Description**
1	**Introduction**	
1.1	Organisational details	Name of organisation, location, areas specifically covered by the plan etc
1.2	Objectives	Key organisational objectives the plan is addressing
1.3	Purpose	Specific purpose of the plan
1.4	Critical business function	Details of the critical business function, process, critical asset etc to which the BCP refers
1.5	Assumptions	Key assumptions made in developing the plan, e.g. availability of key resources, constraints on scope of the plan etc
1.6	Processes	Processes, sub processes etc which comprise the critical business function, or support the use of the asset / facility
1.7	Activation and stand down	Events, outage times, etc which serve as triggers for the activation and deactivation of the BCP. Arrangements, processes etc for activation and stand down
1.8	Responsibility	Names of people with the responsibility for the creation and maintenance of the plan.
1.9	Version control; and maintenance	Version number of the plan, date of creation, date of next review, details of review authorisations, sign off of plan etc
2	**Operational Requirements**	
2.1	Critical success factors	What level of capability the critical business function must achieve
2.2	Interdependencies	Key internal and external dependencies
2.3	Outage times	Minimum acceptable outage times and/or required recovery time for critical processes, functions, resources etc
2.4	Compliance	Compliance requirements which have to be met following activation of the plan (e.g. regulatory, contractual etc)
3	**People**	
3.1	Structure	Structure and reporting relationships of the team operating under the plan
3.2	Roles and responsibilities	Roles and responsibilities of key managers and staff
3.3	Contact details	Business and after hour contact details of key managers, staff, suppliers, customers and other stakeholders, Where possible, key roles and suppliers should have deputies / alternates identified.
4	**Continuity Arrangements**	
4.1	Coordination	Arrangements for coordination between plans and across multiple locations
4.2	Accommodation	Details of alternate / backup site arrangements
4.3	Resources	Types and quantities of resources required to support the activation and implementation of the BCP. Include: • People • Information & documentation • Accommodation • Budget • Assets & other equipment • Telecommunications • IT Systems & applications

		• Plant & property
4.4	Workarounds and alternate solutions	Identify tasks which can still be undertaken following a disruption, the tasks which can't be undertaken and alternate solutions to those tasks to still achieve acceptable outcomes.
4.5	Continuity management tasks	Identify additional activities which have to be undertaken in response to the disruption (other than routine activities). E.g. - assessment of the impact of the disruption, coordination of asset relocation, staff briefings to be held etc
5	**Communications**	
5.1	Communications	Summary of communications requirements following activation of the plan
6	**Appendices**	
6.1	Other plans	Details of other related plans, availability, location and access
6.2	Checklists	Activity checklists e.g. – impact assessment checklists, recovery log sheets etc
6.3	Maps and drawings	Location maps, site maps, layouts etc

This guide has been designed to assist vendors up to and including the development stage. Each vendor should develop and instigate their own exercising process and review / maintenance program to ensure the effectiveness and currency of any strategy or plan which is developed.

FURTHER ASSISTANCE

Should you require further information, there are Industry and professional BC organisations and websites which can provide assistance or further guidance. Some examples include:

• AFGC, Crisis Management Guide:	www.afgc.org.au
• HAL, Horticulture Industry Crisis Management Guidelines:	www.horticulture.com.au
• The Business Continuity Institute:	www.thebci.org.au
• Continuity Central:	www.continuitycentral.com
• Continuity Forum:	www.continuity.net.au

APPENDICES

The appendix contains sample templates (as demonstrated in this document) which can be used for the following tasks:

- Undertaking Business Impact Analysis
- Calculating Minimum Resource Requirements
- Identifying Key Business Dependencies
- Identifying Alternate Workarounds
- Developing Response / Continuity Strategy

Business Impact Analysis						
Process Name & Summary Description	**Worst Case Risk Event / Threat for Process**	**Maximum Tolerable Outage**	**Recovery Time Objective**	**Likelihood**	**Impact**	**Overall Risk Rating**

Minimum Resource Requirements								
Critical Business Function / Process:								
Resources	**Resource Requirements** ***Minimum levels required to complete key business process***						**Normal Resource Level**	**Manual Workarounds (Yes / No)**
	Day 1	**Day 2**	**Day 3**	**1 Week**	**2 Weeks**	**Over 2 weeks**		

Key Business Dependencies

Name of Dependent Party	Supports Critical Process	Tolerable Outage Tine	Impact Summary	Continuity Strategy / Workaround

Alternate Workarounds			
Critical Business Function			
Critical Resource Requirement	**What Critical Tasks / Activities / Processes Can be Performed?**	**What Critical Tasks / Activities / Processes Cannot be Performed?**	**What Alternative Processes or Workarounds Can be Employed?**

Strategy Development Template

Critical Business Process / Function			
Critical Infrastructure			
Risk Scenario			
MTO Time		**RTO time**	
Response requirements			
Response Option 1		CBA	
Response Option 2		CBA	
Response Option 3		CBA	
Response Option 4		CBA	
Recommended Option		**Response Objectives**	
Detailed description of response			
Preparatory requirements		**Responsibility**	