



Divisions of General Practice

Information Management Maturity Framework
(IMMF)

**Toolkit – Business continuity plan
template**



Information Management Maturity Framework (IMMF)

Toolkit – Business continuity plan template

Purpose

The purpose of the “Business continuity plan template” is to assist Divisions to address the action tasks below.

Action Tasks	Capacity Gap	IMMF Element
Develop a business continuity plan addressing the needs of all the Division’s programs and services.	Reactive to Defined	Compliance and Quality

This task should have been identified from the Information Management Maturity Framework (IMMF) gap analysis and toolkit specification.

This tool provides a high level information management (IM) business continuity plan template that can be used to develop a Division’s basic business continuity plan (BCP). This will assist CEOs to effectively manage risks that may arise for Divisions and to progress towards satisfying any BCP or risk management accreditation requirements.

A high level understanding of business continuity planning is a pre-requisite for the use of this tool (refer tool – “Business continuity checklist”).

Knowledge of the business continuity plan template is a pre-requisite for using more advanced tools including:

- Division’s business continuity plan scenarios.
- Guidelines for IM risk management.
- IM guidelines for risk analysis.

Explanatory notes

Business continuity planning requires a Division to identify and understand what are its key business functions and what are the IM resources that are necessary to achieve those functions.

Within a Division, business continuity planning can be described as the process of developing contingency plans and mechanisms to ensure timely information recovery, the restoration of essential records and business resumption in the event of information corruption or loss that may disrupt the Division’s business operations.

The business continuity plan template provides a high level logical structure and a guide to the development of a Division’s BCP.

Key documents - This tool was developed with reference to AS/NZS HB 292-2006 A Practitioners Guide to Business Continuity Management and AS/NZS 4360, Risk management.



Instructional design

This tool consists of one Part – Business Continuity Plan template

Division CEOs should review the guidelines and consider the Division’s IM requirements to enable it to maintain an acceptable level of business operation during periods of unplanned interruptions.

The business continuity plan template is not exhaustive, it is a simple tool that can be used to ensure that the basic business continuity planning process has been initiated and that Division management has considered whatever needs to be done to maintain essential business functions operating if an adverse event occurs. CEOs may find that some elements of the template are not relevant to their Division, while other template elements may require further detail and research.

Business continuity planning is a management issue that requires senior management commitment and involvement. Consequently the business continuity plan template should be discussed and completed with senior staff within a Division.

The completed template should form the basis of a Division’s BCP.

Business continuity planning procedures and policies should be included in the Division’s procedures manual and relevant job descriptions.

Summary of outcomes and resources

Workstreams	Outcomes	Resources
New processes or procedures to be adopted	The business continuity plan template is completed and is used to develop the Division’s IM BCP. The Division’s procedures manual is updated with selected elements from the business continuity plan template.	This tool is self administered by the CEO and senior program staff.



Part 1: Business continuity plan template

General guidelines

A BCP should describe how IM can be maintained at a level that will enable a Division to function at an acceptable level if unplanned adverse events occur.

As a Division's IM capability increases so does its reliance on IT and IM procedures and processes.

A critical step in the BCP process is to consider:

1. Are there adequate procedures implemented to ensure that back-up information can be restored?
2. Can relevant people access that information?
3. Is the integrity of the information maintained?

Testing and measuring the BCP can provide the Division with information regarding the effectiveness of controls and the suitability of its BCP.

Business continuity plan template overview

The template is the first step in developing a BCP. The BCP should list the key actions that will ensure an acceptable level of business functionality will be maintained. The increased reliance on information by Divisions requires that a back-up of data is an essential component of the business continuity plan.

The type of functions that CEOs may consider to be essential includes:

- Ensuring data returns to external stakeholders e.g. Commonwealth and State health authorities can be produced when required.
- Issuing invoices and receipts.
- Managing information systems for patient care (where a Division has direct patient contact).
- Knowing who to contact for technical advice on getting the system operational again.
- Knowing how to restore data using the back-up medium, and together, with technical support to ensure that computer hardware and software are restored to normal working conditions.
- Outlining any of the additional roles that staff might need to undertake while the 'disaster' is active.

A BCP will ensure that when a business disruption, perhaps a catastrophic disaster occurs, the disruption to a Division's services and programs will be kept to a minimum and that resumption of business operations will be as quickly and efficiently as possible.

Business continuity plan template

The suggested business continuity plan template is not exhaustive. The template provides a means to implement the key stages of business continuity identified in the earlier "Business continuity checklist" tool

The stages are:

- Identify critical business functions.
- Identify information resources that are required to support and enable critical business functions.
- Determine recovery method and medium for each information resource.
- Identify all types of resources to be backed-up.
- Determine recovery procedures and policies.

The template is a simple tool that can be used to ensure that the basic business continuity planning process has been initiated and the Division's management has considered what needs to be done to keep essential functions operating if an adverse event occurs. A more comprehensive template can be obtained from "A Practitioners Guide to Business Continuity Management" referenced below.

CEOs may find that some of the templates are not relevant to their Division, while other templates may require further detail and research.



1.1.

1.2. Step 1 - Identify critical business functions

The key consideration is to identify and understand what are the Division's key functions that rely on IM.

Critical Function	Critical success factors	Functional interdependencies	Priority
Eg. Staff Payroll	Payroll must be lodged by the 10 th of each month	IT Functionality including software must be operational	High

1.3. Step 2 – Determine IM resources that are required to support and enable critical business functions (identified in Step 1).

Consider all types of information including, paper, electronic and images as well as soft knowledge.

Critical Function	Resource	Acceptable outage time
Eg continued – Staff Payroll	Data	1 day

1.4. Step 3 – Determine information back-up method and medium for each IM resource (identified in Step 2) in acceptable timeframes for identified risks

1.5.

List current back-up method(s) and procedures and then identify work to be done to enable the recovery of resources within acceptable timeframes. Current procedures in relation to resources will indicate the preparedness or resilience of resources.

Resource (some examples)	Current procedures/comment	Work to be done to satisfy resource recovery requirements
1. Data		
<ul style="list-style-type: none"> Data is backed up on a daily basis 	A daily tape is stored off-site by a specialised organisation (many Divisions use other forms of electronic media)	Back-up data must be restored within 1 day (as detailed in step 2) - Check access time for tape.



		<ul style="list-style-type: none"> - Check hardware will work. - Ensure an adequate maintenance policy exists and is implemented.
2. IT infrastructure		
3. People (IT key personnel)		

1.6.

1.7. Step 4 – Identify all types of resources to be backed-up

Type of file	Files	Completed/comments
System Software (manages and controls computer hardware such as a printer driver)		
Application software (enables users to perform tasks, such as spreadsheets and word processing software)		
User files (user files such as email and word processing files)		

1.8.

1.9. Step 5 – Determine recovery procedures and policies

Back-up procedures and policies should include a list of key people and their responsibilities and a communication plan in the event of an adverse event occurring. Below is a suggested template for each activity.

1.10.

1.11. Identify and list key people who have BCP responsibilities

A key consideration is how to ensure that the information is kept current; a strong link with HR policies and procedures may be beneficial.

	Person – position (examples)	Mobile	Tel.	Responsibility
P1	John Smith – CEO	04xx xxx xxx	02 xxxx xxxx	Person who can declare a disaster, invoke the BCP and declare the disaster has ceased.



P2	Fred Jones – Deputy	04xx xxx xxx	02 xxxx xxxx	Provide support and in the absence of the CEO, make decisions regarding business continuity.
P3	Susan Brown – CIO	04xx xxx xxx	02 xxxx xxxx	Ensure BCP procedures and policies are implemented.

1.12. Develop a communication plan for stakeholders

This is a dynamic document that will need to be kept current as the business and the environment in which it operates changes. A Division will need to determine what are the “trigger points” for each outage.

Name/Group to be notified (Employees, suppliers, stakeholders etc)	Responsible Person	Completed/Comments
Senior Management	P3	
Suppliers	P2	



References and further reading

- AS/NZS 4360:1999 Risk management. Standards Australia August 2004
- HB 292-2006 A Practitioners Guide to Business Continuity Management June 2006
Available at: www.saiglobal.com
Last viewed: April 2008
- Business Continuity Management – Keeping the Wheels in motion (Australian National Audit Office) June 2006
Available at: www.anao.gov.au/uploads/documents/Business_Continuity_Management.pdf
Last viewed: April 2008
- The CPCG Computer Security Self-Assessment Guideline and Checklist for General Practitioners (February 2004).
Available at: www.gpcg.org
Last viewed: April 2008
- Network Resource Library – Australian General Practice Network
Available at: www.agpn.com.au/site/index.cfm
Last viewed April 2008

There is considerable useful material on business continuity and risk management available on the AGPN website.

End of Document