



## Divisions of General Practice

Information Management Maturity Framework  
(IMMF)

**Toolkit – Business continuity  
checklist**



# Information Management Maturity Framework (IMMF)

## Toolkit – Business continuity checklist

### Purpose

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

Action Tasks	Capacity Gap	IMMF Element
Implement business continuity training for key staff	Unaware to Reactive	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 succinct explanation of a business continuity plan (BCP) and its importance in relation to a Division’s ability to continue delivering its services and programs. It also provides a business continuity checklist that can be used as the first step in a Division’s business continuity planning process. This will assist Chief Executive Officers (CEOs) with their general responsibility to manage their Division’s risks and to progress towards satisfying any BCP or risk management accreditation requirements. Divisions need to have a disaster recovery strategy in order to gain or maintain accreditation.

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

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

### Explanatory notes

Business continuity planning requires Divisions to have a formalised approach to identifying and dealing with potential risks and interruptions to business functions and resources.

In relation to IM, business continuity planning is defined as the existence of 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.

Business continuity planning is integral to a Division’s risk management, corporate governance and quality management processes. It has become a focus area for more recent legislation and is mandated for public sector organisations.

The Business continuity checklist provides a simple list of key focus areas that a CEO should consider when implementing a 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, June 2006.

### Instructional design

This tool consists of two Parts:

Part 1 – Business continuity guidelines

Part 2 – Business continuity checklist



**Part 1 – Business continuity guidelines**

The guidelines should be read and discussed with senior staff at the Division, as well as any staff identified as critical to the business continuity planning process. CEOs should also read the tool – “Guidelines for IM risk management”.

CEOs may also discuss business continuity planning with other Divisions to better understand how to approach their BCP and to share any useful business continuity planning related experiences.

The guidelines can then be adapted to create business continuity policies and procedures that should be included in the Division’s procedures manual and in relevant position descriptions for key staff.

**Part 2 – Business continuity checklist**

The business continuity checklist is the first step in the business continuity planning process. The checklist is not an exhaustive list, it is a simple tool that can be used to ensure that a basic business continuity planning process has been initiated and the Division management has considered what needs to be done to keep essential functions operating if a risk event occurs. The checklist is somewhat “information centric” as Divisions’ reliance on information is increasing and there is a greater focus on collecting and disseminating information.

Successful management of information enables Divisions to meet their program and service obligations and improves relationships with practices and other external partners.

CEOs should identify a pilot program or service area within their Division to provide practical experience using the checklist and establishing a BCP.

**Summary of outcomes and resources**

Workstreams	Outcomes	Resources
<p><b>Skills or knowledge acquisition requirements for staff</b></p>	<p>Senior staff are familiar with the definition and stages of business continuity planning.</p>	<p>This tool is self administered by the CEO and senior staff.</p> <p>New processes or procedures may be mentored by Divisions with greater experience in IM business continuity planning.</p>
<p><b>New processes or procedures to be adopted</b></p>	<p>Business continuity planning is initiated in at least one program within the Division.</p> <p>Key staff have business continuity related responsibilities aligned with each stage of business continuity planning.</p> <p>The Division’s procedures manual is updated with selected items from the business continuity checklist and is aligned with the stages of the BCP.</p>	



## Part 1: Business continuity guidelines

Traditionally, business continuity planning (BCP) has focused on IT disaster recovery. However, recent world events highlight the importance of having a well developed BCP that includes maintaining business resilience and long-term performance. This more holistic and proactive approach is referred to as business continuity management.

Business continuity planning is defined in the IMMF as:

*“The existence of 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”*

This is the focus of this tool. However, the processes and procedures can be applied to other key functions of the Division.

Risk management in relation to IM, is a broader concept and relates to the impact of failures in any of the IM workstreams – skills and knowledge, processes and procedures, technology or culture, as they impact on the Divisions performance as specified in the Annual Business Plan. It includes the identification of events and potential disruptions to IM that may affect a Division’s ability to deliver its programs and services. Thus BCP can be seen as a response to one of the key risks identified in a risk management plan.

The key outcome of business continuity planning is to determine what is the minimum level of acceptable performance for an organisation and what IM infrastructure and resources are required to sustain that level.

As a Division’s information maturity increases so does its reliance on IM technology solutions. In addition information back-ups are needed in case information within a file or a group of files is lost. The reasons for losing files include hardware failure, accidental deletion of the wrong file, computer theft and portable storage devices being lost. If information is stored on paper, it can be destroyed or lost in the event of a flood, fire or pest infestation.

A critical step in the business continuity planning process is to ensure that procedures are implemented to enable back-up information to be restored, that relevant people can access that information and the integrity of the information is maintained.

### **What are the key stages of business continuity planning?**

Business continuity planning includes the following key stages (as detailed in Part 2 of this tool – “Business continuity checklist”):

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

CEOs need to consider what is appropriate for their Division and how business continuity planning policies and procedures will be implemented. Business continuity planning requirements may vary between Divisions. For example, larger Divisions may be able to allocate a dedicated resource to develop a BCP while smaller Divisions may need to allocate business continuity planning tasks to several staff.

### **Why does a Division develop a BCP?**

Business continuity planning requires a Division to identify what its key business functions are and what are the necessary resources to achieve these functions. Following a risk identification process, Divisions can then better understand where their business functions are most vulnerable and then identify and implement risk mitigation strategies. For example, as a condition of funding, all Divisions are required to provide National Performance Indicator (NPI) data to the Commonwealth Government. If the data return is not provided on time funding penalties may apply. A key requirement for all Divisions is to ensure they can provide NPI data even in the face of an adverse event, such as a hard disk failure. In this situation back-ups of that data and the capacity to recover it are essential.



Testing and measuring the BCP can provide the Division with information regarding the effectiveness and suitability of its risk management, including controls that mitigate or reduce risk.

### **Who is responsible for business continuity planning within a Division?**

The CEO is responsible for ensuring a Division has a BCP. The CEO and senior management must be committed and provide ongoing leadership to the business continuity planning process.

### **How to better identify potential disruptions?**

A reporting framework needs to be established to ensure that potential and actual disruptions and incidents that may affect business continuity are identified.

CEOs need to promote an internal culture that rewards and recognises incident reporting particularly as staff can be embarrassed or fearful of disciplinary actions that may result from errors or oversights. Divisions need to provide an environment that is conducive to the reporting of any such incidents, along with policies that clearly state how the Division will respond. For example, making incident reporting confidential will require policies and procedures that will give an employee confidence that they will be protected.

Depending on its appropriateness, CEOs should explore ways of sharing knowledge with CEOs of Divisions who have experienced a loss or disruption to information.

Developing a list of known incidents will assist Divisions to identify potential adverse events that could threaten business continuity. A list of known incidents relating to IM could be recorded in an IM issues and improvements register. CEOs should read the Tool – “Guidelines for an IM issues and improvements register”. Periodic review of the IM issues and improvements register will help identify potential threats to business continuity.

### **How critical is information to a Division?**

Increasingly information is becoming a key business resource and an asset that requires management and protection. Much of a Division’s activity centres around collecting and disseminating information.

A successful BCP requires users to have access to information that supports key business activities. This requires a range of functions, such as a suitable back-up procedure and suitable hardware, to be operational.

Divisions also need to consider “soft knowledge”. For example an employee may have in-depth knowledge of a particular GP’s work practices or preferences e.g. being unable to be contacted on Wednesdays due to house calls, or preferring to be contacted by fax. If this employee leaves the Division or is unavailable then this information may be lost to the Division.

To gain an appreciation and better understanding of its information asset, a Division should conduct an inventory of its information (in all its forms), understand its importance in relation to business processes and implement procedures to restore information if it is lost.

### **What are the key risks mitigated by a BCP?**

Information can exist in many forms, including paper documents, images or electronic. It is an asset that requires protection especially as business connectivity increases; exposing information to an increasing and wider variety of risks.

More obvious risks include fire, floods and power disruptions. However, less obvious risks such as a disgruntled employee and sabotage may possibly have more significant consequences for an organisation.

Also less obvious is the information lost due to staff turnover. Loss of a key member of staff can result in a serious loss of information that is critical to the Division’s daily operations.

For further information and guidelines regarding risks refer to the tool – “Guidelines for IM risk management”.



### **What information is critical to a BCP?**

The Division needs to identify all types of information, including paper-based, electronic and other media that are critical to business continuity and ensure they are backed-up. “Soft knowledge” or experience held by key staff should also be considered.

The type of electronic files required to be backed-up, includes the following:

- System software (manages and controls computer hardware such as transferring data from memory to disk)
- Application software (such as spreadsheets, word processes)
- User files (documents, emails, instruction manuals)
- Other files

For each type of electronic file, a decision needs to be made regarding the back-up method, back-up medium and back-up procedures.

### **How are electronic files backed-up?**

In-house back-up of information is the preferred practice of back-up for most Divisions. Larger Divisions may wish to consider the use of off-site backup services. When conducting in-house information back-ups, there are different types of back-up methods and devices that can be employed; factors such as capacity, speed, cost and ease of use will determine the appropriate back-up method.

Below is a list of some devices that can be used to back-up information:

- CD/DVDs. This is an inexpensive option that generally requires no additional hardware or software. Many newer computers come with a built in drive that can copy data directly to CD/DVDs. Read/write (RW) CD/DVDs can be used many times.
- Tape drives. Magnetic or digital tape cartridges can be used to store data. Magnetic tape drives are relatively slow and magnetic tapes can deteriorate which may result in loss of data. However, overall cost of using magnetic tape is less than digital tapes and is a relatively cheap option that is popular with many smaller to medium size organisations. Tape drives, while still in use, are becoming obsolete and are being progressively replaced by portable hard drives.
- Portable (external) hard drives or disks. In comparison to the options above, these devices are able to store a very high amount of data and offer speed advantages, which is important during storage and retrieval of data. However the total cost of this option is higher when compared to other options.
- USB flash drives. The functionality of a USB flash drive, i.e. speed and access of data, is similar to a computer hard disk. USB flash drives plug directly into a computer’s USB port, are relatively low in cost and can hold a relatively large amount of data. However, USB flash drives are prone to being lost (misplaced), are difficult to label and have a higher failure rate than other media. This method is not recommended for any purpose except for a short-term interim measure.

Procedures and processes regarding back-ups need to be developed and implemented. For example, the frequency of back-ups and off-site storage facilities need to be determined.



## Part 2 - Business continuity checklist

Below is the business continuity checklist. It is not meant to be an exhaustive list but is intended to provide users with a list of key focus areas for consideration when developing their BCP.

The list is an ongoing process that needs to be reviewed on a regular basis.

### **Business continuity checklist**

#### **Identify critical business functions**

- Identify the minimum level of acceptable performance for the Division.
- Identify the infrastructure and resources that are required to achieve and sustain the minimum level of business operations.
- Determine stakeholder expectations of acceptable service delivery.
- Assess the likely future scenarios that may result in a disruption to the Division's services and programs.
- Identify communication requirements including channels.

#### **Identify information resources that are required to support and enable critical business functions**

- Conduct an "Information Inventory" to identify all the information needed to maintain required functionality.
- Consider all types of information including, paper, electronic and images, and soft knowledge.
- Determine what information is critical to business functions.

#### **Determine back-up method and medium**

- Photocopy, scan or digitise images of paper based records.
- Determine how to back-up electronic information (e.g. magnetic tape, CDs, off-site facilities etc).

#### **Identify all types of files to be backed-up (including)**

- System software.
- Application software.
- User files.

#### **Determine back-up procedures and policies**

- Develop back-up policies in relation to IT.
- Plan what to do in case of emergency.
- List key personnel and their responsibilities.
- Develop a communication plan.
- Implement a testing and review cycle for the BCP.



## 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](http://www.saiglobal.com)

Last viewed April 2008

Business Continuity Management – Keeping the Wheels in motion

(Australian National Audit Office - January 2008)

Available at: [www.anao.gov.au/uploads/documents/Business\\_Continuity\\_Management.pdf](http://www.anao.gov.au/uploads/documents/Business_Continuity_Management.pdf)

Last viewed April 2008

Network Resource Library – Australian General Practice Network (AGPN)

Available at: <http://www.agpn.com.au/site/index.cfm>

Last viewed April 2008

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

**End of Document**