



Divisions of General Practice

Information Management Maturity Framework
(IMMF)

**Toolkit – Guidelines for IM risk
management**



Information Management Maturity Framework (IMMF)

Toolkit – Guidelines for IM risk management

Purpose

The purpose of the “Guidelines for IM risk management” is to assist Divisions address the action tasks below.

Action Tasks	Capacity Gap	IMMF Element
Implement an IM risk management program	Reactive to Defined	Management

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

This tool will assist (Chief Executive Officer) CEOs to more effectively manage information management (IM) risks that may impact on the delivery of a Division’s programs and services. This tool also provides high level guidelines to CEOs to enable them to develop a process to identify and mitigate IM risks focusing on projects within the Division. Using this tool will also help to meet accreditation requirements.

Knowledge of the “Guidelines for IM risk management” is a pre-requisite for using more advanced tools including:

- IM guidelines for risk analysis.

Explanatory Notes

A uniform approach to IM risk management requires Divisions to adopt a standard definition of risk management and to adopt a formalised approach to identifying and dealing with potential risks and interruptions to business activities that may affect service outcomes. This will enable CEOs to improve their overall IM to help ensure that their Division continues to deliver its Business Plan outcomes through the identification of IM risks that may impact the Division’s programs and services.

A risk management methodology requires a Division to identify, prioritise and manage risk events to an acceptable level in a cost-effective manner.

At a high level, the risk management methodology provides a logical structure and guide to the development of a Division’s risk management procedures.

Risk management has strong links to business continuity planning and information security. Applying risk management techniques to IM will result in greater safety and security of a Division’s information resources.

Key documents - This tool was developed with reference to AS/NZS 4360, Risk Management.



Instructional Design

This tool consists of one Part – Guidelines for IM risk management

Guidelines for IM risk management

CEOs should review the guidelines, specifically using the risk management framework, to determine the Division’s requirements in relation to IM risk management.

The guidelines should be read and used for training senior staff of the Division, as well as any staff identified as critical to the risk management process.

An initial IM risk analysis should be done using the Division’s current Annual Business Plan. Repeatable procedures and policies should be included in the Division’s procedures manual and relevant job descriptions. CEOs should seek advice from other Divisions or SBO staff for advice on how other Divisions and other comparable organisations have implemented and confirmed adherence with IM risk management procedures.

Summary of outcomes and resources

Workstreams	Outcomes	Resources
Skills and knowledge	<p>Staff are trained and are aware of the IM risk management framework.</p> <p>Senior staff are able to apply IM risk management procedures to the activities and outcomes specified in the Division’s Annual Business Plan and also for projects initiated outside the plan.</p>	<p>New skills and knowledge is to be self administered within a Division.</p>
New processes or procedures to be adopted	<p>A formal IM risk analysis is routinely completed as part of the Division’s business plan.</p> <p>The Division’s procedures manual is updated with selected items from the IM risk management guidelines.</p>	<p>This tool is mentored for the implementation of new processes.</p>
Culture and change management requirements	<p>Risk management responsibilities are implemented in selected staff job descriptions.</p> <p>Staff apply IM risk management procedures to the activities and outcomes specified in the Division’s Annual Business Plan and also for projects initiated outside the plan.</p>	<p>Mentoring by CEOs of Divisions that have demonstrated a capacity for IM risk management.</p>



Part 1: Guidelines for IM Risk Management

Overview

The guidelines are intended to assist CEOs and staff at Divisions to identify, prioritise and manage risk as a key part of the way they plan, manage and monitor their business activities. Risks need to be managed for each activity or outcome in the Division's Annual Business Plan.

The guidelines outline the basic principles of IM risk management and provides two basic templates. The first template can be used to identify business outcomes and associated risks against the four workstreams of the IMMF. The second template can be used to prioritise risks and can be used as a basis for a risk log.

The focus of this tool is on IM risk management but it could be used across the Division's other functions and resources.

IM risk management is similar to general risk management in that both relate to planning and dealing with adverse events. However, they differ in that IM risk management focuses on the Division's IM plans and activities whereas general risk management relates to adverse events that affect the Division's overall ability to deliver its programs and services. General risk includes IM risk as well as a wider range of risks such as an extended power failure or a fire.

What is IM risk management and what is its purpose?

IM risk management is defined in the IMMF as:

"The mechanisms for identifying, measuring and monitoring relevant IM risk for the Division's business plans and activities, including options for risk allocation and risk mitigation".

For example, a breach of privacy will impact on relationships with general practitioners. This is one risk Divisions must manage when handling confidential data.

The purpose of IM risk management is to ensure that the Division's business objectives are more likely to be achieved and that damaging outcomes will not, or are less likely to, happen.

What is the relationship between business continuity and IM risk management?

In the IMMF, business continuity refers to the timely recovery of essential records and business resumption in the event of information corruption or loss and is therefore a response to one specific area of risk. IM risk management is a broader concept and includes all IM risks that may impact the Division's business plans and projects.

IM risk management should consider all areas of risk and all the likely consequences of a risk event occurring. For example, the reputation of a Division may suffer if a software application that the Division installs onto a general practice computer system crashes the system. In addition IM risk management should consider National Performance Indicator (NPI) data and funding consequences that may be at risk due to IM failure.

IM risk framework

The IM risk framework should provide a Division with a comprehensive approach in identifying, prioritising and managing IM risks which have the potential to impede or stop the Division achieving its business or service outcomes or NPI requirements.

IM risk management can be approached by considering the impact of failures in any of the IM workstreams; skills and knowledge, processes and procedures, technology or culture; as they impact on the Division's performance as specified in the Division's Annual Business Plan.

Focus areas will include a Division's key business activities or outcomes that have a high dependence on IM. Trivial or minor IM risks should be removed and excluded from further analysis.



Following on from the example above, an identified requirement in the Division's Annual Business Plan is to ensure the timely lodgement of NPI data. This outcome can be assessed against the four workstreams of the IMMF.

Risk management techniques (further discussed below) can then be applied to each risk to ensure that the outcomes are more likely to be achieved. Below is a suggested template using the example above.

Template 1: Risks to achieving outcomes.

Key business outcome or activity	IM Workstreams	Risks	Risk Management
Timely lodgement of NPI data	Skills and Knowledge	Staff are not trained to use the PHCRIS data entry system	Ensure more than one staff member is trained each year
	Processes and procedures	Procedures for collecting Practice data not documented	Document the processes for how each data element is collected from practices
	Technology Solutions	NPI Data is lost and is not included in back up procedures	Test BCP annually using a lost NPI data scenario
	Culture	Staff lack enthusiasm for NPI reporting, thus failing to meet set deadlines	Run staff training to ensure all staff understand the link between NPI reporting and funding

Risk Identification

For risk management to be effective, it is critical that all important risks are identified and understood. Possible risks for Divisions include damage to relationships with members arising from a breach of confidentiality, not being able to meet reporting requirements and not identifying issues or concerns of members quickly enough. As discussed, one approach is to identify risks against the four IM workstreams of the IMMF. This approach can be strengthened by using risk identification techniques such as brainstorming, reviewing case studies and discussing risk related issues with other CEOs or SBO staff. IM risks may also be identified by staff using an IM issues register.

Prioritising Risks

Table 1 below is an example of a matrix table that can be used to prioritise risk events. The range of consequences and / or likelihood of events, as well as the categorisation of risk events, can be simplified or expanded to better suit a Division's needs.

The likelihood and consequences of a risk event needs to be examined from the perspective of possible consequences with existing controls (discussed below) in place and possible consequences if these controls weren't in place.

For example, (refer Table 1 below) a risk event that has a "Rare" likelihood and would have a "Minor" consequence for a Division is categorised as a low risk "L" and can probably be managed by routine procedures. Alternatively, an event such as a building fire or flood may be considered to have a 'rare' likelihood but the associated 'Catastrophic' consequences categorises this risk as 'Extreme' and therefore requires immediate action.



Table 1: Categorisation of risk events based on likelihood and consequence

Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost certain	L	M	H	E	E
Likely	L	M	H	H	E
Possible	L	M	H	H	E
Unlikely	L	L	M	H	E
Rare	L	L	M	H	E

Legend

- E: Extreme risk; immediate action required
- H: High risk; senior management attention needed
- M: Moderate risk; management responsibility must be specified
- L: Low risk; managed by routine procedures

An example of a risk, 'loss of data' is contained in the suggested template (Template 2: Risk categorisation and associated actions) below. The template can be used to prioritise risks that are identified in the risk framework and can be used to initiate a 'risk log' that should identify ownership and status of risks.

Template 2: Risk categorisation and associated actions

Risk	Likelihood	Consequence	Categorisation	Action	Comment
Data is Lost	Unlikely	Catastrophic	E	Immediate	The urgent requirement for a business continuity plan will be raised immediately with senior management.

Controls

Controls refer to the process of implementing and maintaining appropriate management controls including policies, procedures and practices to reduce the effects of risk to an acceptable level.

When assessing the best option for treatment of IM risks Divisions should consider the cost of implementing controls as some controls may have high costs that offer little benefits to a Division. For example, a control to reduce the risk of computer failure could be to have spare desktop computers available but this would be a costly control for a Division. A better treatment of the risk may be to have a plan developed to be able to quickly source and purchase a new computer if the need arises.

Controls in risk treatment can be categorised as:

- Prevention - Prevent or reduce impact to the information environment from an action or event occurring.
- Detection - Provides notification that something has gone wrong.
- Correction - Has the ability to correct identified problems.
- Deterrence - Avoid or prevent an undesirable event.

Monitoring

Risk monitoring is a key stage of risk management as it provides information regarding the effectiveness and suitability of techniques and procedures. The key steps of risk monitoring include the following:

- Check that execution of the planned actions is having the desired effect.
- Watch for early warning signs.
- Model trends predicting potential risks.
- Check that the overall management of risk is being applied effectively.



Project management and risk

IM risk management, as part of project management, focuses on IM risks that may affect the project goals being achieved on time and within budget. The IM risk management techniques discussed above can be adapted and used in managing project risks.

Limitations of risk management

Risk management does not guarantee that adverse events will not occur; it is about planning and dealing with these events to minimize disruption to business functions. Risk management is a process and consequently the effectiveness of outcomes will depend on the quality of the inputs and the thorough application of risk management processes.



References and further reading

- AS/NZS 4360:2004 Risk management Standards Australia, August 2004.
- HB 292-2006 A Practitioners Guide to Business Continuity Management, June 2006.
- HB 436-2004 Risk Management Guidelines - Companion to AS/NZS 4360:2004, August 2004.

Accessed at: www.saiglobal.com

Last viewed: April 2008

Australian General Practice Network (AGPN) Network Resource Library

The AGPN Network Resource Library is an extensive clearing house of information serving GPs and the Divisions. It does contain reference material relevant to risk management. Access to much of the material requires a logon ID and password – CEO login can be obtained from webmaster@agpn.com.au.

Website: www.agpn.com.au.

End of Document