



Divisions of General Practice

Information Management Maturity Framework
(IMMF)

Toolkit – IM guidelines for risk
analysis



Information Management Maturity Framework (IMMF)

Toolkit – IM Guidelines for Risk Analysis

Purpose

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

Action Tasks	Capacity Gap	IMMF Element
IM risk analysis is routinely completed as part of the IM plan.	Defined to Managed	Management

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

This tool is intended to raise the Division’s level of information management (IM) governance to support proactive risk management through a formal and systematic approach to information security and IM governance. The guidelines will assist Chief Executive Officers (CEOs) to systematically manage IM risks that may impact on the delivery of a Division’s programs and services.

This tool also highlights the increasing legal and compliance requirements and provides some practical examples relating to IM risk. Using this tool will also help Divisions meet accreditation requirements.

Knowledge of the “Guidelines for IM risk management” is a pre-requisite for using this tool. It is also a pre-requisite for using this tool that the Division has developed an IM plan that defines IM outcomes for each of the Division’s programs and services.

Explanatory Notes

As described in “Guidelines for defining IM outcomes” and “Guidelines for IM risk management”, the Division’s IM outcomes that support and enable the achievement of the Division’s programs, requires risk to be managed through a risk management methodology that is part of a Division’s IM governance framework.

A proactive approach to IM risk management requires well developed information security policies and procedures that specifically relate to the health sector and particularly, IM governance. There needs to be a regular risk analysis and review of the impact of risk against IM outcomes to ensure that risks are identified and addressed. IM risk management should also be part of day to day activities for all staff.

IM risk analysis will enable CEOs to further improve their overall IM capability which will improve the likelihood of a Division being able to deliver its Annual Business Plan outcomes in a timely manner and will reduce the possibility of legal and / or compliance issues.

Risk analysis has strong links to business continuity planning and information security. Applying risk analysis and 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 HB 174-2003 Information Security Management, implementation guide for the health sector and AS/NZS 4360, Risk Management.



Instructional Design

This tool consists of one Part – IM guidelines for risk analysis

CEOs should review the guidelines and examples to determine the Division’s requirements in relation to proactive IM risk analysis. CEOs should ensure that risk analysis procedures are consistent with the Division’s IM risk management framework and are implemented on a day to day basis across the Division.

The guidelines and examples should be read and used for training relevant staff within the Division.

CEOs should seek advice from other Divisions or State Based Organisation (SBO) staff on how their Divisions or other comparable organisations have implemented and confirmed adherence with IM risk analysis procedures.

Summary of Outcomes and Resources

Workstreams	Outcomes	Resources
Skills and knowledge	<p>Senior staff are able to apply proactive risk analysis procedures to the Division’s IM Plan and to IM projects or programs.</p> <p>Comprehensive risk reporting and response procedures are implemented.</p>	<p>New skills and knowledge is to be self administered within a Division.</p>
New processes or procedures to be adopted	<p>A risk governance framework is established and implemented.</p> <p>There are formalised processes and procedures for dealing with IM security incidents.</p> <p>IM risks are prioritised, monitored and reported regularly.</p> <p>The Division is committed to continuous improvement in managing risk.</p>	<p>This tool is mentored for the implementation of new processes.</p>
Culture and change management requirements	<p>Senior staff ‘lead’ improvement through policies, procedures and by example.</p> <p>A culture of honesty and trust through a ‘no blame’ reporting system is established.</p> <p>Staff implement risk analysis procedures as part of their day to day activities.</p>	<p>Mentoring by CEOs of Divisions that have demonstrated a capacity for IM risk management.</p>

IM Guidelines for Risk Analysis



Definition

Risk analysis: Accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information.

Overview

CEOs and relevant staff at Divisions need to identify, prioritise and manage risk as a key part of the way they plan, manage and monitor their business activities including managing risks for each activity or outcome in the Division's Annual Business Plan.

The increasing need and ability to store, retrieve and send sensitive health information electronically is raising the importance of information security and IM governance for health industry organisations.

Proactive risk analysis should occur within an IM risk framework and specific attention should be paid to information security and IM governance. These topics are the focus of this tool and will enable CEOs to manage risks more efficiently, achieve business outcomes and reduce the risk of facing legal actions or compliance issues.

IM risk framework

A Division's IM risk framework should provide a comprehensive approach to identifying, prioritising and managing IM risks that have the potential to impede or stop the Division achieving its business or service outcomes or National Performance Indicators (NPI) requirements.

As described in the tool "Guidelines for IM risk management", IM risk management can be approached by considering the impact of failures in any of the IM workstreams as they impact on the Division's performance as specified in their Annual Business Plan. A similar approach could be taken in relation to IM risk analysis (refer IM governance below) which forms part of an organisation's information security policy and procedures.

Some key risk areas identified by Divisions include:

- meeting contract commitments;
- patient information being divulged to unauthorised parties or being incorrect;
- reporting what has been done;
- managing funding sources;
- securing funds;
- maintaining a good reputation*;
- high turnover of staff; staff not documenting their knowledge;
- having multiple programs and reporting bodies; and
- using outside contractors.

* Example: There was an instance of a pharmacist not disclosing records to anyone, including the CEO of the relevant Division, due to a lack of trust of Division staff.

IM Governance

A key area in relation to analysing and managing risk is IM governance as it provides the operational framework and the procedures to be implemented on a day to day basis.

IM governance involves what decisions must be made to ensure effective IM, who should make these decisions and how decisions will be made and monitored. IM governance will change over time and will vary between Divisions.



Table 1 contains examples of some governance activities under each of the IM workstreams.

Table 1

Key business outcome	IM workstreams	Governance activity (example)
IM governance	Skills and knowledge.	All staff are trained in risk management.
	Processes and procedures.	Risk management processes and procedures are standardised and implemented across the Division.
	Technology solutions.	The Division uses antivirus and other protective software.
	Culture.	Acceptable IM operating standards are achieved through training.

The above table can be expanded to include other relevant governance activities or IM risk outcomes.

IM governance will be primarily determined by a Division’s information security policy and procedures.

Information security

Information security is extremely important to organisations as information is a strategic asset. For organisations operating in the health industry, the security of information is critical.

A breach of information security in the health sector may be life threatening for a patient and have legal or other compliance consequences, such as funding implications. Consequently, health information security is a broader term that includes protecting and safeguarding patient information and privacy. In addition, health information security should ensure that relevant information is accurate and available when required.

Information security is primarily achieved by implementing a set of controls which may be a policy, procedure or technology solution. HB 174-2003 – Information security management, implementation guide for the health sector (www.saiglobal.com) is a set of guidelines that details controls which may be considered best practice in health information security. Relevant key areas of the guidelines include, the following:

- All organisations need to have an understanding of their risks, vulnerabilities and consequences to enable security requirements to be addressed (refer to the tool “Guidelines for IM risk management”).
- Health information is increasingly being stored and transmitted electronically. Organisations need to have an information security policy that details IM security principles and compliance requirements.
- Organisations should include IM security and privacy responsibilities in their job descriptions.
- There needs to be regular IM security education, training and awareness (including information privacy and confidentiality).
- There need to be methods for dealing with IM security incidents.
- Data should not be vulnerable to unauthorised and unexpected change or modification and is backed-up regularly.



Legal/compliance requirements

There are several Commonwealth and State Acts that relate to the health sector including the Privacy Act 1988, Electronic Transactions Act 1999 and the Privacy Amendment (Private Sector) Act 2000 (for further examples, refer to HB 174-2003).

CEOs should be mindful that legislative requirements may not be intuitive and that the definitions and concepts may be broader than every day use. For example, the Privacy Act requires sensitive information to be safeguarded and states that other types of 'sensitive information' includes information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, professional or trade association membership, union membership, sexual preferences or practices, or criminal record (refer - The National Privacy Principles and Health – Protecting privacy throughout the information life cycle www.privacy.gov.au).

It is therefore important that staff training adequately addresses legal and compliance requirements. The following is an extract from a case study (www.privacy.gov.au/act/casenotes/ccn12_06.html) that highlights the importance of adequate training and education.

“...when contacted by the complainant, the health service provider stated that the disclosure was inappropriate and was made by a new employee who understood that the results of tests should not be disclosed, but did not realise that the types of tests undertaken should also not be disclosed.”

Monitoring

Risk monitoring is a key stage of risk management as it provides information regarding the effectiveness and suitability of risk analysis techniques and procedures. The frequency of reviews will vary between Divisions and will be influenced by the type of business activities. Reports, both formal and informal, may be another indicator of the requirement to review risk management procedures.



References and further reading

- HB 174-2003 Information security management Standards Australia March 2003.
- 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
Available at: www.saiglobal.com August 2004.
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 most of the material requires a logon ID and password – CEO login can be obtained from webmaster@agpn.com.au

AGPN website: www.agpn.com.au

End of Document