Victorian Government Guideline
Information Management

Information Management Roles and Responsibilities

Guideline

This guideline provides advice for information management governance and custodianship responsibilities.

Keywords:	Information management, custodianship, information ownership, information asset management.		
Identifier: IM/GUIDE/01	**Version no.:** 1.1	**Status:** Final	
Issue date: 1 July 2012	**Date of effect:** 1 July 2012	**Next review date:** 30 June 2014	
Authority: Victorian Government CIO Council	**Issuing authority:** Victorian Government Chief Advocate	Technology	

DEPARTMENT OF PREMIER AND CABINET
State Government Victoria

Contents

Overview

This document provides guidance to Victorian Government departments and agencies establishing or reviewing their information management responsibilities and governance.

Audience

This guideline has been developed for the 11 Victorian Government departments and the following agencies: Victoria Police, VicRoads, State Revenue Office, Environment Protection Authority and CenITex. The guidelines can be used by any interested agency.

The guideline is specifically targeted at officers involved in managing information or governing information management programs. This includes:

- chief information officers (CIO);
- chief information security officers (CISO);
- senior line-of-business representatives with significant information assets under their management;
- information management specialists;
- information owners;
- information custodians; and
- information security officers.

Rationale

1.1 Why information is important

Government is largely a knowledge-based industry and can only operate efficiently and effectively when staff and citizens have access to the right information.

Key drivers for information management programs include:

- responding to legislative requirements;
- managing information security risk;
- improving service delivery through information sharing or business intelligence;
- improving reporting and analysis;
- promoting transparency and open access; and

- reducing costs by minimising duplication, management and storage.

1.2 Information management principles

The Victorian Government has recognised the need to improve and better coordinate its information management practices and the Victorian Government Information Management Principles have been adopted to guide these improvements:

1. Information is recognised as a valuable asset.
2. Significant information assets are managed by an accountable custodian.
3. Information meets business needs.
4. Information is easy to discover.
5. Information is easy to use.
6. Information is shared to the maximum extent possible.

Information assets

1.3 What is a significant information asset?

The *Victorian Government Information Asset Custodianship Standard* (IM/STD/01) defines a significant information asset as a discrete collection of data or information, stored in any manner, which is recognised as valuable to the organisation.

Individual agencies are responsible for determining which information assets are considered valuable in their organisational context. However, agencies should consider the following criteria:

- Legislation mandates that the asset be maintained and/or accessible.
- A sensitive asset could cause damage or legal consequences if accessed or used inappropriately.
- A loss of integrity of the asset would compromise the agency's operations, harm commercial entities or members of the public.
- A loss of availability of the asset would compromise the agency's operations, harm commercial entities or members of the public.
- A contract or memorandum of understanding with an internal or external party would be breached if the asset was unavailable or its integrity compromised.
- The asset is recognised as a significant public knowledge asset.

An information asset can be in electronic or hard copy format and can include:

- text files;
- web content;

- unstructured data;
- structured data;
- spatial data;
- documents;
- tables;
- electronic messages;
- metadata; and
- images.

1.4 Register of information assets

Advice on how to establish and maintain an information asset register will be provided in the Victorian Government Information Asset Register & Metadata Guideline. This will include a recommended metadata profile for use in registers.

1.5 Critical information asset register

Identification of critical assets is a key step for agencies developing their Information Security Management Framework. Critical information assets are a subset of the significant information assets held by an agency. Therefore, a current and well-maintained information asset register should provide the starting point for identifying critical assets.

More advice on the identification of critical assets can be found in the WoVG information security policy, standards and guidelines.

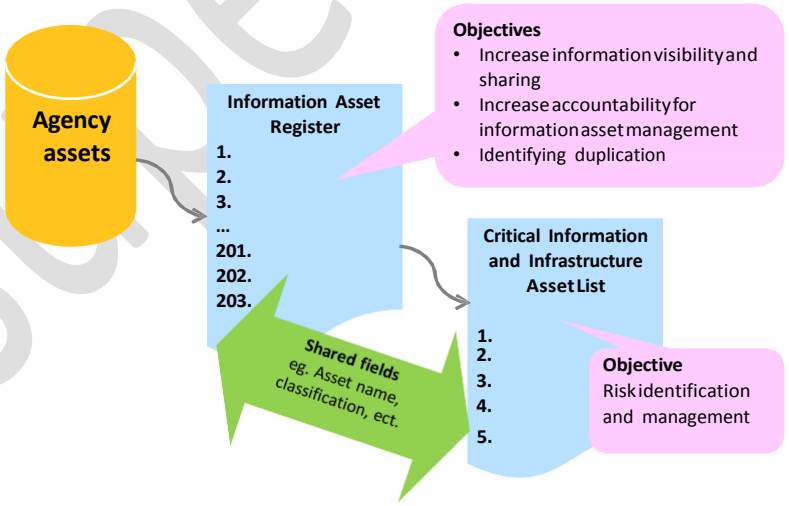


Figure 1: Information asset register and critical information asset list

1.6 Information types

When identifying an agency's information asset, it can help to think about the information types. Data and information can be categorised into four major content types: transactional, analytical, authored and published.

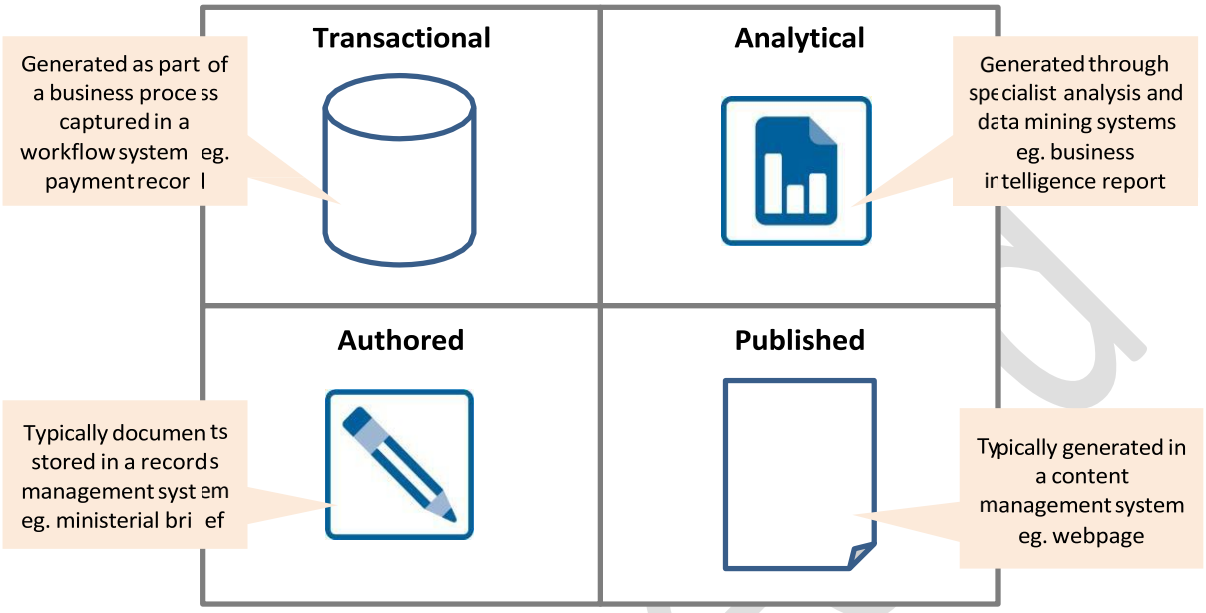


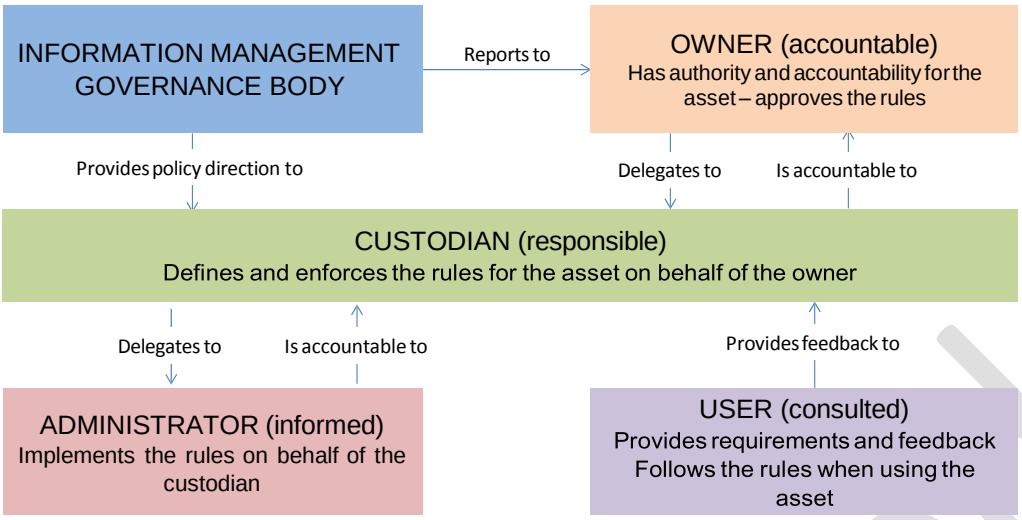
Figure 2: Information types (Adapted from Information Content Types Fact sheet, Queensland Government Enterprise Architecture, February 2011)

Transactional and analytical information is structured and typically stored in a database. Authored and published information is more often semi-structured or unstructured.

Roles in information management

Individual agencies are responsible for developing and implementing a custodianship, an agency specific custodianship model which articulates key responsibilities in the management of significant information assets. Outlined below is a recommended custodianship model which encompasses five key roles:

- owner;
- custodian;
- user;
- administrator; and
- governance body.



Adapted from *Information management roles and responsibilities*, The State of Queensland (Department of Public Works) 2011 and *Ownership Model Across Business and IT*, Department of Human Services, Victoria

Figure 3: Information asset register and critical information asset list

1.7 Information owner – accountable officer

Under the Financial Management Act[1], the department head or agency chief executive officer has ultimate responsibility over the agency's asset and risk management, including information risk.

Information owners approve the rules associated with an information asset.

In practice, the accountable officer may delegate responsibility of information assets to a delegated owner who in turn delegates to an information custodian.

Typically the accountable officer will retain responsibility for:

- approving the agency's information management and technology (IM&T) strategy; and
- approving forward work plans and supporting business cases relating to IM&T investments.

1.7.1 Delegated owner

The delegated owner has authority and accountability for the information asset. They are typically a divisional director or line of business lead. For example, the director of human resources (HR) may be the delegated owner of employee information within their agency.

[1] Financial Management Act 1994, Victorian Consolidated Legislation, http://www.austlii.edu.au/au/legis/vic/consol_act/fma1994164/

1.8 Information custodians

An information custodian is a nominated individual who is formally accountable for managing the delegated assets in their care. Custodians direct how the information is managed and used on behalf of the owner.

Custodians should have strong business knowledge of the information asset and will typically be a subject matter expert in the subject matter covered in the information asset. For example, the HR Manager responsible for recruitment might be the custodian for employee information within their agency.

In many cases a custodian will not be an information technology or information management expert. In some cases, they may not be directly involved in maintaining or supplying information. These activities may be delegated to an administrator.

The information custodian is responsible for:

- registering the information asset;
- working with the information owner to classify the information asset according to its security level;
- ensuring information asset quality is in line with business needs;
- ensuring information is discoverable, including the maintenance of metadata;
- ensuring information is easy to use by adopting common standards where possible; and
- ensuring information is shared to the maximum extent possible in accordance with security and statutory requirements.

Each information asset should have one custodian.

1.8.1 Registration

All significant information assets must be registered in the agency's information asset register. Custodians should register assets once created or acquired. Agencies may also wish to register planned assets to help identify duplication before any investment is made.

1.8.2 Classification

VG information security policies and standards require that information assets are classified according to their security level. Agencies are required to nominate an information owner or an appropriate senior manager to be accountable for the protection of each significant asset. That person is to be recorded in the inventory of significant assets and is responsible for ensuring the appropriate marking of assets, defining and reviewing access controls, and other information security controls.

Custodians should work with the information owner to ensure the information asset is managed in accordance with its security level.

1.8.3 Quality

The way that information is developed and managed should be based on its strategic importance. Therefore, custodians should:

- work with users to determine information needs;
- consider information use as the information is being collected or developed; and

- manage, maintain and communicate information quality.

When choosing to reuse an existing information asset, users need to assess if it is fit for purpose. A key factor in this decision is often data quality. A data quality statement is an effective mechanism for communicating information about how data can be used.

1.8.3.1 Data quality tools

The Australian Bureau of Statistics (ABS) Data Quality Framework provides the standards for assessing and reporting on the quality of statistical information. It helps users decide whether a dataset or statistical product is fit for purpose, assess the data quality of seemingly similar collections, and interpret data.

The framework can be used to:

- define a data need;
- declare quality of your own, or another organisation's data item or collection of data items (quality statements);
- compare your data need with available data (identification of data gaps); and
- design a collection (this may be a result of the identification of data gaps).

The VPS Data Integrity Manual was developed with the aim of increasing capability and awareness of data integrity across the public sector and to assist VPS entities to better manage their data. It includes the following:

- a consistent framework for describing data quality in terms of completeness, consistency, validity, accuracy, timeliness/availability;
- a data integrity impact assessment questionnaire to help custodians understand data needs; and
- guidance on the types of data integrity controls which should be considered.

1.8.4 Discoverability

For government to function effectively, the public, government employees and partner organisations must be able to find the information they need. However, access to some information must be restricted due to security, privacy, confidentiality or commercial risks.

Custodians are responsible for providing and maintaining metadata so that information can be found.

Agencies are already required to comply with the *WoVG WMF Standard: Discoverability* which helps citizens find information and increases website discoverability through internal and external search engines. Requirements include implementing descriptive and meaningful values for the mandatory and recommended properties of the AGLS Metadata Standard (AS 5044-2010) on all web pages.

1.8.5 Usability

Applying agreed standards to information makes it easier to use and interpret. Standards help to determine how information will be collected, described, defined, stored and shared.

Custodians should:

- work with users to determine appropriate standards;

- work with other custodians to identify common standards; and
- adopt common standards where possible.

WoVG Data Standards and Guidelines provide advice on the use of agreed standards including address data standards.

1.8.6 Sharing

The more an information asset is used, the more its value increases.

Sharing information assets across government:

- reduces burden on organisations providing information;
- reduces the overall cost of information development and management; and
- improves collaboration and creates a more connected government.

Information sharing with the public:

- promotes government transparency;
- stimulates innovation and commercial activity; and
- gives researchers access to more primary data.

Custodians should ensure that:

- information is collected, developed, stored and maintained with sharing, collaboration and interoperability in mind;
- information sharing is facilitated and actively promoted;
- information is shared in accordance with security and statutory requirements; and
- users build on existing information rather than re-collecting or re-creating information.

1.8.7 Why custodianship?

The term custodianship has been used as it reinforces two key concepts:

- information assets should be actively cared for; and
- while one person or organisation may take on the role of caring for an information asset, it is likely to be of value to a broader audience.

In some organisations, the title ‘custodian’ has been interchanged with ‘steward’ or ‘owner’.

Custodianship in action: Victorian Spatial Council

The Victorian Spatial Council (VSC) Custodian Program provides a formal methodology and technical environment for release of spatial information, through which companies, agencies and government departments can confidently share their location/geographic information via a secure and controlled environment.

Through the Custodianship Program, an organisation acknowledges that it is the single authoritative source for a dataset and agrees to take appropriate care in the collection, storage and maintenance of the information.

A framework of standard agreements manage issues such as copyright and liability. A database enables on-line search and description of datasets. Standard distribution channels ensure that users receive updates whenever they are issued and custodians know and control who is using the data.

Provided security agencies classify information assets before entering the custodianship program, the VSC framework covers the requirements of the Victorian Government Information Asset Custodianship Standard.

1.9 Information administrator

An information administrator handles the day-to-day maintenance of an information asset based on the rules set out by the custodian. Information administrators can include outsourced providers.

1.10 Information user

Information users play a key role in information management. They provide requirements and feedback and follow the parameters set by the information custodian. Information users can include staff across government, delivery or research partners and members of the public.

1.11 Legal ownership

Most information assets will contain copyright material. Copyright is a form or intellectual property (IP). The Victorian Government may not own all of the information that it uses or holds. Owning an information asset is not a criterion for including it in an agency information asset register or assigning a custodian to the asset. However, ownership considerations may prevent the information asset from being shared with third parties.

1.12 Shared information assets

Where information assets are jointly owned by multiple organisations, agencies should formally document custodial responsibilities in an agreement.

Information management governance

Central governance within agencies is needed to ensure coordination, visibility and appropriate sponsorship of information management activities. An IMGC provides a mechanism to ensure agency information management efforts are streamlined and coordinated across the agency.

The agency information management governance body must report to the agency head and set overall policy direction for information management.

Sample terms of reference have been included in Appendix A.

1.13 Responsibilities of the IMGC

The IMGC is responsible for the following activities:

- providing leadership in information management in line with Victorian Government information management principles;
- building organisational capability in information management;
- monitoring and reporting compliance with Victorian Government information-related standards;
- ensuring coordination across information-related functions including privacy, freedom of information and information security; and
- providing input into Victorian Government information priorities via the DSLG, CIO Council and its reference groups.

1.14 Providing leadership

An effective mechanism for providing leadership in information management is via a strategy and annual works program. The IMGC should direct their preparation, endorse them and oversee their implementation.

An information management strategy:

- defines the strategic direction for the use and management of information as a valuable asset;
- supports the agency's overarching business strategy; and
- includes performance indicators.

1.14.1 Records management strategy

PROV Strategic Management Standard (PROS 10/10) and supporting specifications require agencies to develop an executive-endorsed records management strategy, which is integrated with other relevant management strategies and is appropriate to agency needs, corporate culture, technological environment and risk exposure. This strategy must be developed, implemented, resourced and assessed for improvement on an annual basis and should be considered as part of the agency's broad information management strategy.

1.14.2 Information security strategy

WoVG information security standards require agencies to provide clear direction on information security through the development and implementation of an agency information security policy, and address agency information security requirements as part of the agency security plan. Again, the policy and plan should be considered as part of the agency's broad information management strategy.

1.15 Building capability

Agencies should ensure that all employees who create, process or handle information have a clear understanding of their agency policies and procedures and of their responsibilities.

Education and awareness programs will likely vary across an agency and between agencies and will depend on the type of work and types of information dealt with.

However, establishing and communicating the agency's custodianship framework and custodianship roles and responsibilities is a key task for all IMGCs.

PROV Strategic Management Standard (PROS 10/10) and supporting specifications require agencies to develop and implement a stakeholder engagement model to ensure stakeholders are informed of recordkeeping requirements.

Similarly, WoVG information security standards require agencies to publish and communicate their information security policy to all employees as appropriate.

1.16 Victorian Government information related standards, coordination and compliance

When developing an information management strategy and plan, agencies must consider a number of information-related legislation and standards including:

- Freedom of Information Act 1982;
- Victorian Public Records Act 1973 and standards;
- Victorian Information Privacy Act 2000;
- Victorian Health Records Act 2001;
- Commissioner for Law Enforcement Data Security Act 2005;
- WoVG information security standards;
- VG Information Management Standards; and
- VG Data Standards.

A key role of the IMGC is to ensure activities within these areas are well coordinated.

Compliance against PROV standards and Victorian Government information management standards will be measured though one coordinated maturity survey. Victorian Government information management priorities

The CIO Council sponsors a Victorian Government information management works program delivered by the Victorian Government Information Management Group and supported by the Digital Government, Department of State Development and Business Innovation (DSDBI).

Agency IMGCs should regularly exchange information with these bodies through their respective representatives.

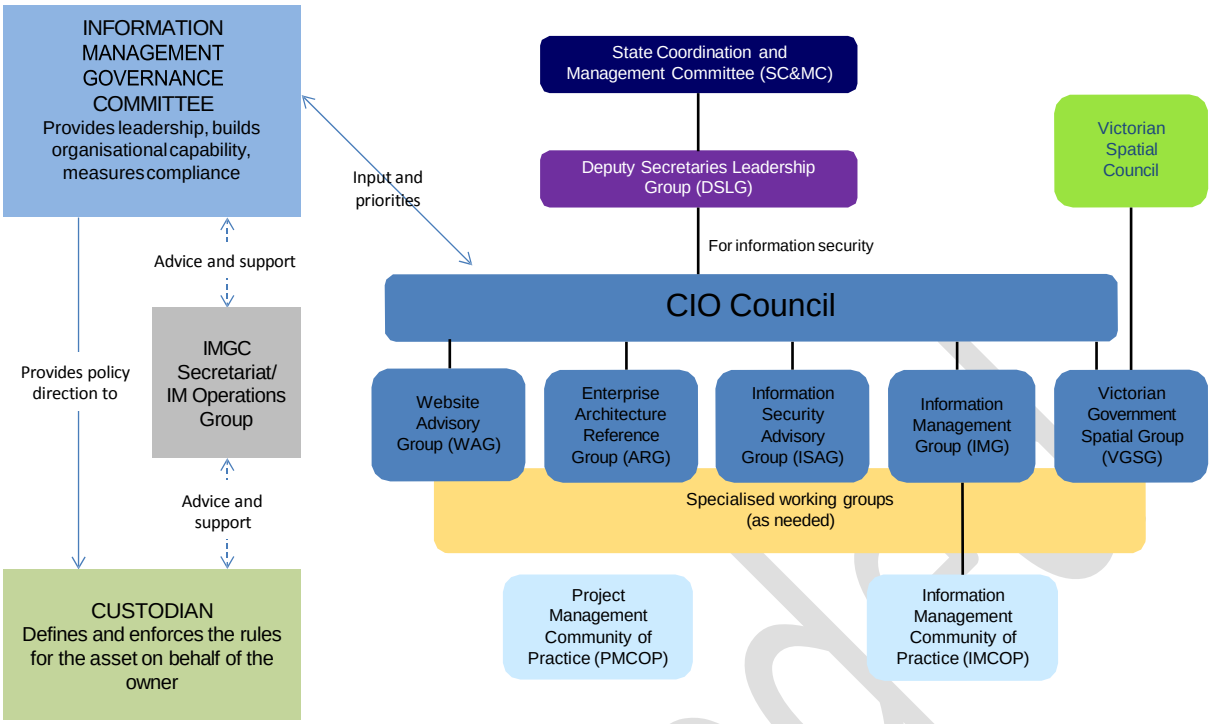


Figure 4 IMGC and VG Information Governance

Derivation

This standard is derived from:

- VG Information Management Principles (IM/GUIDE/00);
- VG Information Management Agency Information Roles and Responsibilities; and
- VG Information Management Information Asset Custodianship.

References and toolkits

Victorian Government standards:

- http://www.enterprisesolutions.vic.gov.au/business-systems/
- Information Management Roles and Responsibilities Guideline (IM/GUIDE/01)

Further information

For further information regarding this standard, please contact the Department of State Development and Business Innovation, at enterprisesolutions@dpc.vic.gov.au

Glossary

Term	Meaning
Information management	The way in which an organisation plans, identifies, creates, receives, collects, organises, governs, secures, uses, controls, disseminates, exchanges, maintains, preserves and disposes of its information. It is also the means through which the organisation ensures that the value of that information is identified and exploited.
Information security	Those measures concerned with ensuring the confidentiality, integrity and availability of information. Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimise business risk and maximise value of the information and services provided to the Victorian community.
CIO Council	Chief Information Officers' Council. The CIO Council reports via the DSLG to the State Coordination and Management Committee (SC&MC) on information security activities.
VG	Victorian Government
Interoperability	The ability of organisations to share data and information and to integrate information and business processes by use of common standards. Interoperability can be achieved by the application of a framework of policies, standards and guidelines that leave decisions about specific hardware and software solutions open for individual agencies or groups of agencies to resolve.
Metadata	Structured information that describes, explains, locates or otherwise makes it easier to discover, retrieve, use or manage an information asset.
Confidentiality	Ensuring that information is accessible only to those authorised to have access
Integrity	Safeguarding the accuracy and completeness of information and processing methods.

Version history

Version	Date	GSD TRIM ref	Details
0.1	30 April 2012	D11/222825	Initial draft.
1.0	2 July 2012	D11/ 222825	Final
1.1	July 2013		Template update

Appendix A: Sample IMGC terms of reference

Introduction

This document contains the terms of reference for Information Management Governance Committees (IMGC).

Role of the IMGC

The role of the IMGC is to lead, monitor and report on information management activities.

The IMGC is responsible for:

- providing leadership in information management in line with Victorian Government (VG) information management principles;
- building organisational capability in information management;
- monitoring and reporting compliance with VG information-related standards;
- ensuring coordination across information-related functions including privacy, freedom of information and information security; and
- providing input into VG information priorities via the Deputy Secretaries Leadership Group (DSLG), CIO Council and its reference groups.

Member roles

Chair

The IMGC must is chaired by an executive-level officer.

The role and responsibilities of the Chair are to:

- call meetings for the IMGC on a periodic basis;
- set the agenda for each IMGC meeting and disseminate the meeting agenda and supporting documentation prior to the scheduled meeting;
- serve as a moderator for each IMGC meeting;
- call subject matter experts to attend IMGC meetings as required; and
- ensure that the IMGC meeting's objectives are fulfilled.

Members

The IMGC includes the following functional representation:

- agency CIO (or equivalent);

- chief information security officer (CISO); and
- senior line-of-business representatives with significant information assets under their management.

The responsibilities of members are to:

- attend meetings or delegate a representative;
- ensure that delegates are adequately briefed and able to provide value to the IMGC;
- participate actively in the meetings and all decision-making activities;
- propose agenda items;
- proactively support, act and assist to promulgate the decisions made by the IMGC; and
- be collectively accountable for the delivery of the agency's information management strategy and outcomes.

Secretariat

The IMGC is supported by a Secretariat function led by a senior information management officer. The Secretariat assists the Chair to set the agenda, disseminate supporting documentation and prepare minutes.

The Secretariat is also responsible for the operational management of the agency's information management works program.

Meeting management

Decision-making process

When possible, decisions should made by consensus.

If, after some effort consensus cannot be reached by the members, then a favourable vote of 70% or more of all voting members may pass an IMGC meeting decision. Each member will have one vote.

Motions for a vote may be made and seconded only by members of the IMGC.

Six IMGC members must be present to reach quorum.

Voting rights are transferable to a delegated representative.

Frequency and duration

The meetings will be held quarterly or as required. Meeting duration is approximately 60 minutes.

Attendance

Members may delegate a substitute attendee, but members are expected to not miss more than two consecutive meetings.

Agendas

IMGC members wishing to place agenda items should advise the Chair at least seven working days prior to each meeting.

The meeting agenda and agenda papers will be provided to members at least five working days prior to each meeting

Standing agenda:

- previous minutes;
- action items;
- progress against the agency information management works program;
- updates to government-wide information-related policies;
- other business.

Minutes

Minutes and action items are be documented by and distributed to attendees within seven working days.

Governance

The IMGC reports to the agency head.

Communicates with and provides advice, feedback, as required, to:

- DSLG;
- CIO Council;
- VG Information Management Group; and
- other agency IMGCs (as required for networking purposes) .