# Information Management Governance Guideline

## Information Management Framework

Premier and Cabinet

# Document controls

## Approval

This document was approved by the CIO Leadership Group on ## <Month> 2017, and applies from the date of issue (see below).

| | | | |
|---|---|---|---|
| **APPLIES TO** | All Departments and Victoria Police | **AUTHORITY** | Information Management Group |
| **PERIOD** | 2017 – 2020 | **ADVISED BY** | Enterprise Solutions<br>Department of Premier and Cabinet |
| **ISSUE DATE** | 02/08/2017 | **DOCUMENT ID** | IM-GUIDE-06 |
| **REVIEW DATE** | 02/08/2020 | **VERSION** | 1.0 |

## Version history

| Version | Date | Comments |
|---|---|---|
| **0.1** | 30/05/2017 | First draft |
| **0.2** | 04/07/2017 | Final draft incorporating IMG feedback. |
| **1.0** | 02/08/2017 | Approved |

# Contents

# Introduction

## Overview

This document provides high level guidance to Victorian Government departments for implementing the *IM-STD-03 Information Management Governance Standard* (the standard) and for establishing or reviewing their information management governance processes. This document is a guide only.  The requirements listed at the top of each section are a copy of the requirements detailed in the standard.

In this guideline, ‘information’ means information, records or data.

## Rationale

Government operates efficiently and effectively when staff and citizens have access to the right information.

Information management governance is about the ownership and decision rights around information. It is about maturing information management practice and creating a culture that ensures managerial oversight is in place to properly manage and maintain information assets.

Implementation of better information management governance will ensure:

- government information is managed in line with statutory and administrative obligations,
- government information supports and aligns with business drivers, business needs and strategic objectives,
- improved ownership and accountability regarding government information,
- increased capacity of government information to be used and valued as an operational and strategic asset, and
- government information is managed according to its purpose and associated risk profile.

## Derivation, audience, glossary and related documents

### Derivation

This guideline is derived from:

- *IM STD 01 WoVG Information Asset Custodianship (superseded)*
- *IM STD 02 Agency Information Management Governance (superseded)*
- *IM GUIDE 01 Information Management roles and Responsibilities (superseded)*

## Audience

This guideline has been developed for Victorian Government departments and Victoria Police, which are in scope for implementation of the standard, however the content may be of relevance to other agencies.

This 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 and records management specialists
- Information owners
- Information custodians
- Information security officers
- Data analysts.

## Glossary

The glossary of terms and abbreviations used in this document are defined in the IM GUIDE 03 Information Management Glossary.

## Related documents, tools and references

- *DataVic Access Policy*
- *DataVic Access Policy Guidelines*
- *Freedom of Information Guidelines*
- *IM-STD-03 Information Management Governance Standard (awaiting approval)*
- *Public Record Office of Victoria (PROV) Standards Framework and Policies*
- *Victorian Protective Data Security Framework (VPDSF)*
- *Whole of Victorian Government Intellectual Property Policy*
- *WoVG Information Management Framework*
- *WoVG Information Management Policy (awaiting approval)*

# Guidelines

## Executive-level officer

1. Appoint an executive-level officer to champion the importance of information and its management across the department. (e.g. CIO or similar).

An executive-level officer responsible for championing the importance of information and its management provides leadership in maximising the value of information and creating a culture where information is valued as an asset. They would:

- advocate for the improvement of information management practice
- create opportunities for information innovation, reuse, repurpose, integration, transformation and insight
- ensure information management activities are aligned with organisational strategic objectives and business needs
- have oversight of, or work closely with, information management, records management, data management and data insight (analytic) functions.

The requirement for the officer could be met by establishing a new role or by making changes to an existing position. Where appropriate, for example in smaller departments, the responsibilities may be assumed by an existing executive-level role.

## Custodianship model

2. Document a custodianship model that clearly articulates key accountabilities and responsibilities for the management of information, records and data within the department.

4. Nominate a senior information management professional to represent the department at the whole of Victorian Government (WoVG) Information Management Group (IMG).

5. Establish and maintain an internal Information Management Governance Committee (IMGC), or similar, that leads, monitors and reports on information management activities. The IMGC should be chaired by an executive-level officer, report to the department head (or a peak executive body chaired by the department head) and have representation from key business areas.

### Custodianship

> **Custodianship**
>
> *"1. a person who has custody; keeper; guardian.*
>
> *2. a person entrusted with guarding or maintaining a property; janitor."*[1]

[1] Custodian, Dictionary.com, 2017, http://www.dictionary.com/browse/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.

## Custodianship model

Departments must develop a custodianship model that articulates key roles and responsibilities in the management of its information. A custodianship model will ensure:

- accountability for the department’s information (information, records and data),
- that information is managed in a consistent and controlled manner,
- management of compliance to statutory and administrative obligations,
- optimisation of the value of the information as an operational and strategic asset, and
- cost savings in the creation/collection, management and use of information.

Outlined below (see Figure 1 - Example custodianship model) is an example custodianship model that encompasses five key roles:

- Information Management Governance Committee (or a similar governance body)
- Owner
- Custodian
- Administrator
- User

Departments should design their custodianship model to suit their organisational needs. However, at a minimum, departments should ensure that each information asset has an assigned owner (or similar) and custodian (or similar).

The custodianship model (and the key roles) identified is only an example. As long as the requirements of the standard are met departments may choose to define their own job titles, roles and responsibilities.

## Information management governance committee

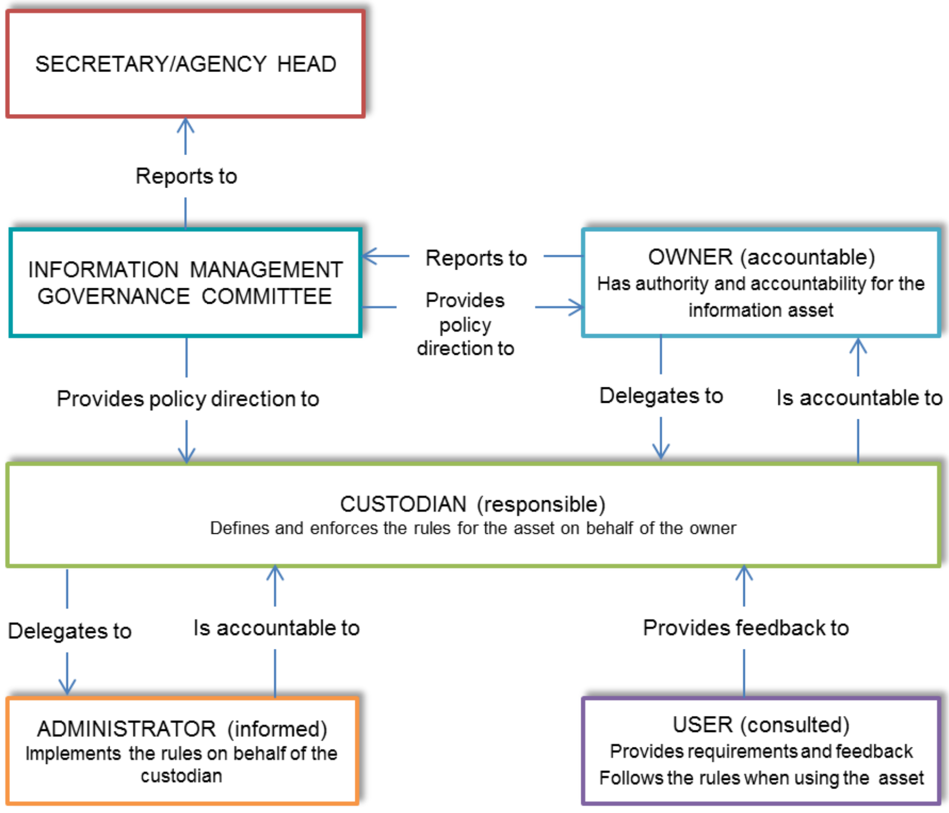
Central governance within departments is needed to ensure coordination, visibility and appropriate sponsorship of information management activities. An Information Management Governance Committee (IMGC), or similar, provides a mechanism to ensure department information management efforts are streamlined and coordinated across the department.

The department IMGC should be chaired by an executive level officer, report to the department head, and include the Chief Information Officer, Chief Information Security Officer and senior line-of-business representatives with significant information assets under their management. The IMGC is responsible for:

- providing leadership in information management in line with the Victorian Government's (the government's) Information Management Framework, Information Management Policy and associated standards,
- setting overall policy direction for the department's information management,
- building organisational capability and capacity in information management,
- putting in place the mechanisms, processes and cultural changes that result in the proactive release and sharing of information assets as applicable,
- monitoring and reporting compliance with government and department information-related policies and standards,
- monitoring and reporting compliance with statutory and administrative obligations,
- ensuring coordination across information-related functions including privacy, freedom of information and information security, and
- providing input into government information priorities via the government's Information Management Group (IMG), the CIO Leadership Group and related reference and working groups.

The department IMGC should nominate a senior information management professional to represent the department at the IMG.

See Appendix A: Sample IMGC terms of reference.


SECRETARY/AGENCY HEAD
Reports to
INFORMATION MANAGEMENT GOVERNANCE COMMITTEE
Reports to
Provides policy direction to
OWNER (accountable)
Has authority and accountability for the information asset
Provides policy direction to
Delegates to
Is accountable to
CUSTODIAN (responsible)
Defines and enforces the rules for the asset on behalf of the owner
Delegates to
Is accountable to
Provides feedback to
ADMINISTRATOR (informed)
Implements the rules on behalf of the custodian
USER (consulted)
Provides requirements and feedback
Follows the rules when using the asset

Adapted from *Information management roles and responsibilities*, The State of Queensland (Department of Public Works) 2011

**Figure 1 - Example custodianship model**

## Owner

Under the *Financial Management Act*[2] the department head or agency chief executive officer has ultimate accountability for the department's asset and risk management, including information assets and risks.

In practice, the accountable officer (owner) 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 department's Information Management Strategy, and
- approving forward work plans and supporting business cases relating to information management investments.

### Delegated Owner

The delegated owner is the executive level officer accountable for management of a specific information asset, ensuring the asset is accurate, current, protected, accessible, and shared and released where applicable. The owner:

- ensures information is compliant with legislation and administrative requirements,
- monitors and controls usage, access and availability of information; authorising or denying access as applicable,
- ensures information quality is improved upon and maintained, and at a stated level of quality,
- puts in place the mechanisms, processes and cultural changes that result in the proactive release and sharing of the information asset as applicable,
- ensures information assets are shared and released to the maximum extent possible, and
- champions the use of the information asset in their business area, department and across government.

The delegated owner need not be directly involved in maintaining or supplying the information but should be in a position to direct such activities and make decisions in line with business processes, business rules, and statutory and administrative obligations.

The delegated owner may choose to delegate his/her tasks to another executive level officer or the custodian, however the owner still has overall accountability for the information. The delegated owner would typically be a divisional director or line of business lead. For example, the directors of human resources may be the delegated owners of employee information within their department.

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

## Custodian

The custodian is appointed by the owner or delegated owner and is formally responsible for managing the information asset in his/her care on a day to day basis. Custodians guide how the information is managed, protected 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 by the information asset. For example, the HR Manager responsible for recruitment might be the custodian for employee information within their department.

A custodian is generally not an information technology or information management expert. In some instances, a custodian may not be directly involved in maintaining or supplying the information. These activities may be delegated to the administrator.

At a minimum the custodian should be responsible for:

- registering the information asset in the information asset register and maintaining associated metadata,
- working with the owner to classify the information asset according to its security level (see the Commissioner for Privacy and Data Protection's (CPDP) *Victorian Protective Data Security Framework (VPDSF)* and risk profile,
- ensuring information assets are created, managed and in accordance with PROV's *Standards and Specifications* and the *Whole of Victorian Government Intellectual Property Policy,*
- ensuring the protection of the privacy of personal information (see CPDP's What is privacy?),
- ensuring information asset quality is in line with user and business needs ('fit for purpose'),
- ensuring information is discoverable and accessible,
- ensuring information is easy to use by adopting common standards where possible, and
- ensuring information is shared and released to the maximum extent possible.

The role of custodian is particularly important when the information asset is owned by an external organisation but used, managed and/or produced by the department. In this instance the custodian acts on behalf of the external owner, ensuring that the information asset is used according to its licensing or contract of use.

## Administrator

The information administrator (not to be confused with a database administrator) is a person with a hands-on information management role and detailed knowledge of the information. They are responsible for the day to day activities to ensure their information asset is of high quality and compliant with information management standards, statutory and administrative obligations. The administrator also plays a pivotal role in the development and execution of data management and data quality management plans. The administrator reports up to the custodian.

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

### User

Users are the individuals or groups who use the information; they play a key role in information management. They provide requirements and feedback and follow the parameters set by the custodian. Users can include staff within the department or across government, delivery or research partners and members of the public.

## Legal ownership and intellectual property

Most information assets will attract intellectual property (IP) protection and owners should, in particular, evaluate whether the Victorian Government or a third party owns copyright prior to sharing or releasing information assets.

Unless there is a good reason not to do so, agencies should grant rights to their IP to the greatest extent possible. The *Whole of Victorian Government Intellectual Property Policy* and supporting *Guidelines* provide the State's framework for the ownership and management of its IP and for its use of IP belonging to other parties.

> The term 'intellectual property' refers to the set of legal rights that protect the results of creative efforts including literary, artistic and scientific works, performances, broadcasts, inventions, scientific discoveries, trademarks and designs.

The State is not entitled to grant rights to IP owned by a third party unless there is an agreement securing all necessary rights. For example, where the IP was created by a third party under a funding agreement or in the course of procurement, the ownership of the IP is typically dealt with under an agreement between the parties and there may be a licence granted to the State.

Departments should be mindful that there may be multiple IP owners associated with an individual asset. For example, the State normally owns copyright in a report prepared by a department, but such a report may also contain an image subject to third party copyright, or background material which already existed and has been contributed by a consultant.

With regard to State IP, a department may only grant rights to IP if it is the department responsible for the IP in question or it has been authorised by the responsible department. The responsible department is clearly best placed to determine the appropriate terms on which to grant rights to IP, and to manage it after doing so.

There are a number of contexts in which it may be appropriate to grant rights to IP, including where:

- a third party requests permission to make use of the State's IP,

- a procurement or funding agreement requires particular uses of the State's IP. For example, a contract to maintain a State-owned ICT system would likely require the contractor to gain a licence to use relevant IP in the system,
- a department develops an invention or innovation that would benefit the public, and
- a department develops useful copyright material.

In these circumstances, the department should assess whether rights to the IP should be granted, by reference to the IP Policy and Guidelines. Assistance may be sought from the department's IP Coordinator, legal division, or from the Department of Treasury and Finance at IPpolicy@dtf.vic.gov.au.

# Strategic leadership

3. Ensure information and data considerations are included in enterprise and divisional strategic planning and document an enterprise Information Management Strategy (IMS)

## Strategic alignment

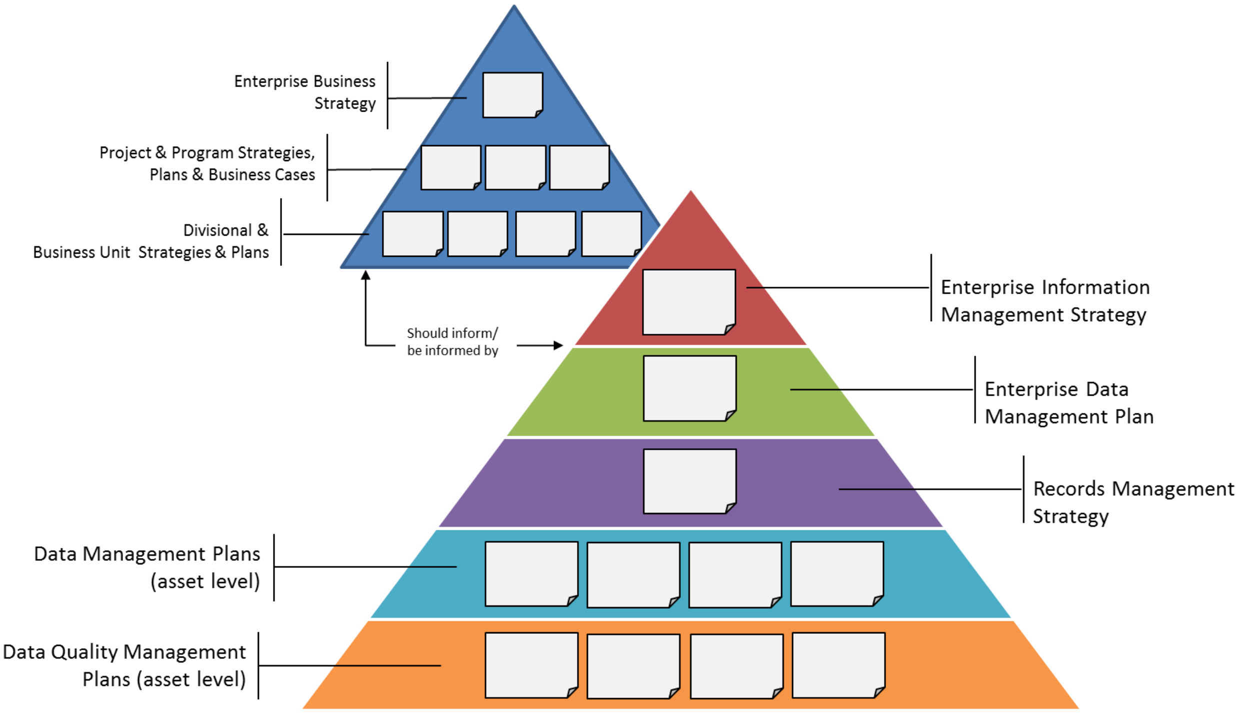

Enterprise Business Strategy
Project & Program Strategies, Plans & Business Cases
Divisional & Business Unit Strategies & Plans
Should inform/ be informed by
Enterprise Information Management Strategy
Enterprise Data Management Plan
Records Management Strategy
Data Management Plans (asset level)
Data Quality Management Plans (asset level)

Figure 2 - Strategic alignment

The benefit of investment in information management usually isn't found in information management itself but rather in how the department's information aligns with and helps to deliver its strategic objectives.[3] As such, information management practice should not be an isolated activity but rather interwoven into business activities and strategic planning.

[3] The Business Case for Information Management, Oracle, December 2008http://www.oracle.com/us/products/middleware/bus-int/064320.pdf

The department's business strategy, project and program strategies, plans and business cases, and divisional and business unit strategies and plans should inform (and be informed by) the enterprise information management strategy, the enterprise data management plan, the records management strategy and asset level plans (see Figure 2 - Strategic alignment).

See the *Enterprise Data Management Plan Standard and Guideline* for the minimum requirements on creating an enterprise data management plan.

## Enterprise information management strategy

### Enterprise information management:

> *"….is an integrative discipline for structuring, describing and governing information assets across organizational and technological boundaries to improve efficiency, promote transparency and enable business insight."*
>
> **Gartner** [4]

Critical to the success of enterprise information management is strategically planning how information is created (or collected), managed, improved and used, as well as how it is aligned with or supports the strategic objectives of the department and government.

An enterprise information management strategy (EIMS) is about whole of department (enterprise) information management leadership, planning and prioritisation. An EIMS establishes information as an operational and strategic asset that supports business functions and key business imperatives.

An EIMS could include:

| Topic | Description |
|---|---|
| Vision and objectives | • Defines the department's information/information management vision and objectives. |
| Current state | • Assesses what the current state of the department's information and enterprise information management is: what works (strengths), what doesn't work (weaknesses) and what's missing (see Information Management Maturity Measurement for self-assessing maturity).[5] |
| Future state | • Documents what the future state of the department's information and enterprise information management might be (may provide examples of best practice and potential options). |
| Governance | • Articulates enterprise information management governance business rules (including the custodianship |

[4] IT Glossary, Gartner, 2017, http://www.gartner.com/it-glossary/enterprise-information-management-eim

[5] Current state versus future state analysis should consider people, process and technology

| Topic | Description |
|---|---|
| | model). |
| Statutory and administrative obligations | • Identifies the statutory and administrative compliance requirements, such as freedom of information, security, privacy and records management, that the department must build into the way that they manage their information. |
| Strategic initiatives | • Identifies strategic initiatives to establish or enhance information management capability and maturity and align information and information management practice with business need and strategic objectives. |
| Capability and capacity | • Determines the capability and capacity required to deliver on the enterprise information management strategy and to improve department information management practice. |
| Implementation | • Provides an information management programme of work implementation roadmap and/or plan. |

Departments may incorporate these elements into an existing document, or use a more business appropriate title if they choose.

The IMGC should direct the EIMS preparation, endorse it for Secretary approval and oversee its implementation.

### 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 department 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 department's broad information management strategy.

## Information Management Maturity Measurement

6. Agencies must participate in PROV's Information Management Maturity Assessment Program (IMMAP) by self-assessing their IM maturity using the IM3 tool every two years.

The Information Management Maturity Measurement (IM3) tool has been developed by PROV to help Victorian Government departments and agencies assess the maturity of their information management practices.

Every two years PROV will ask departments (via the IMG) to carry out an assessment using the tool as a part of a broader assessment of information maturity.

Departments may choose to carry out an assessment on a more frequent basis to support the development and ongoing management of their enterprise information management strategy.

# Information asset registers

7. Implement a department Information Asset Register (IAR) that:
   a. registers all significant information assets
   b. identifies and flags all critical information assets
   c. is accessible to all staff within your department
   d. assigns each information asset an owner and custodian (or equivalent)
   e. complies with the Information Asset Register Standard (under development)
   f. complies with Part II of the Freedom of Information Act 1982.
8. Contribute to the WoVG Information Asset Register.[6]

Significant and critical information assets must be identified and registered in the department's information asset register (IAR) to facilitate discovery, accessibility, protection, and the management of assets throughout their lifecycles.

The following guidance provides high level support for the requirements 7 and 8 of the standard. For more detailed support around identifying information assets and developing and maintaining an IAR see the CPDP's guidance *Information Security Management Collection (Chapter 1, Identifying and Managing Information Assets)*.

## Information assets

**Information Asset:**

*A body of information defined and practically managed so it can be understood, shared, protected and used to its full potential. Information assets support business processes and are stored across a variety of media and formats.*

*Information assets have a recognisable and manageable value, risk, content and lifecycle.* **IM GUIDE 03 Information Management Glossary**

The government has a large investment in information and needs to ensure that it is treated and valued as an asset.

Information assets are essential to the government's decision-making, policy development and service delivery. Like other assets, information needs to be managed, protected and leveraged throughout its lifecycle and maintained as an operational and strategic asset.

Information assets identified as having enduring value to government and/or the community must be transferred to the PROV when the department or agency no longer requires ready access to them.

[6] The WoVG Information Asset Register is a requirement under the proposed Data Sharing Legislation. It is flagged for development in 2017/2018. The WoVG Information Asset Register will be internal to government and have access limited to Victorian Public Sector staff.

## Information asset types

When identifying a department's information assets 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 (see Figure 3 - Information types).

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

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.

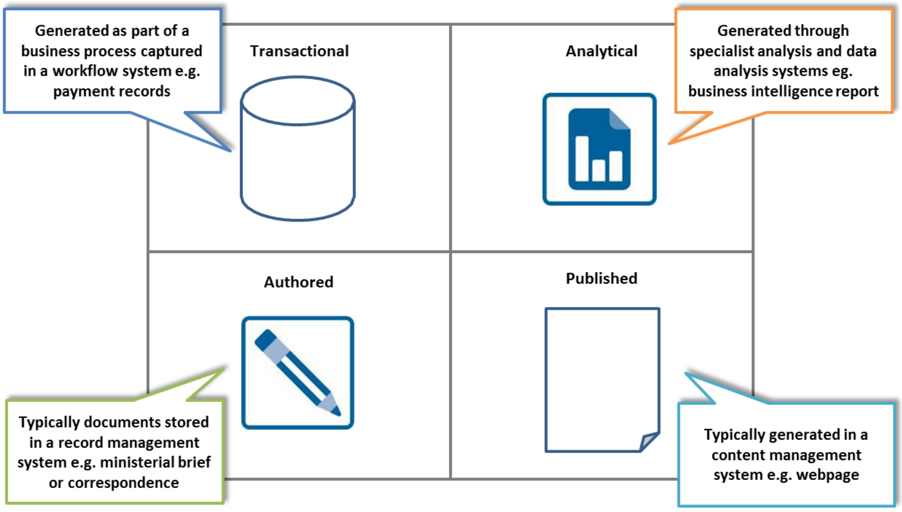

Generated as part of a business process captured in a workflow system e.g. payment records
Transactional
Analytical
Generated through specialist analysis and data analysis systems eg. business intelligence report
Authored
Published
Typically documents stored in a record management system e.g. ministerial brief or correspondence
Typically generated in a content management system e.g. webpage

**Figure 3 - Information types**

Information assets 'types' are just one way of identifying information assets.  You can also identify information assets by function, process, longevity, sensitivity, legislation, where it is stored (system etc.), risk or subject etc.

## Significant information assets

A **significant information asset** is a discrete collection of data or information that is recognised as valuable to the organisation (see Figure 4 – Information assets above). Departments are responsible for determining which information assets are considered valuable in their organisational context, however the following significant information asset criteria may be useful:

- legislation mandates that the information asset be maintained and/or accessible
- the information asset is sensitive and could cause embarrassment, damage or legal consequences if accessed or used inappropriately
- a loss of integrity or availability of the information asset would compromise the department'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 information asset was unavailable or its integrity compromised

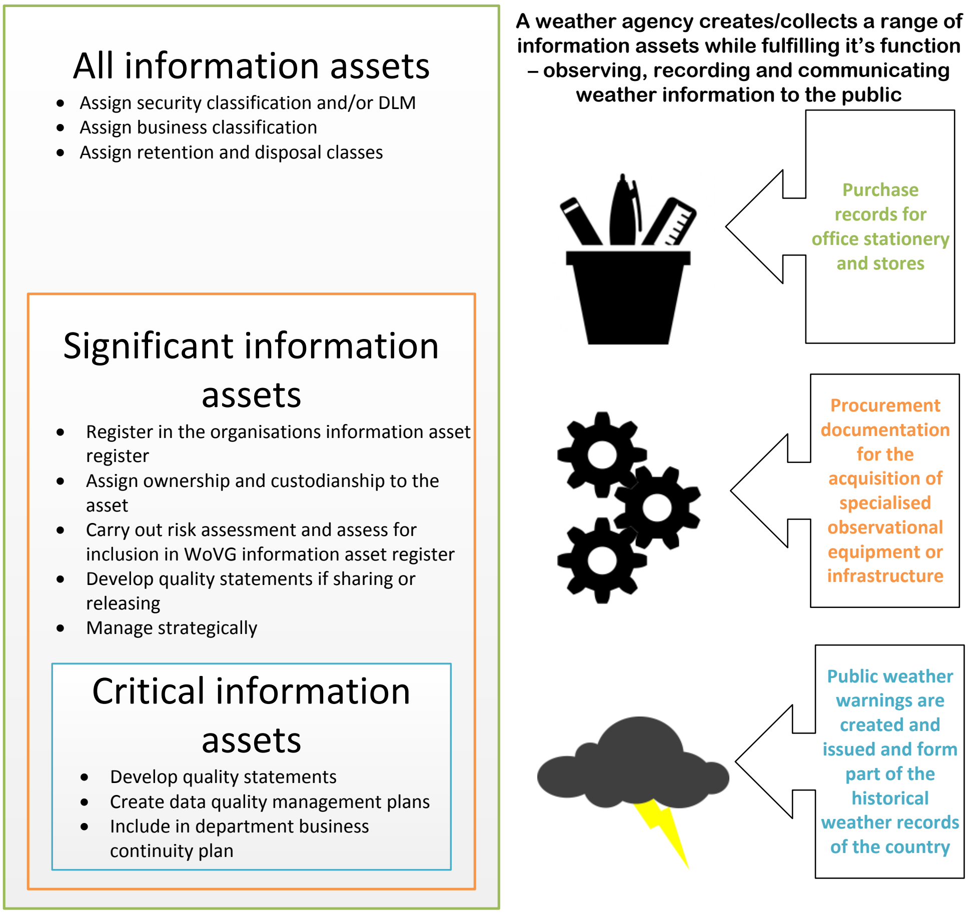

All information assets
Assign security classification and/or DLM
Assign business classification
Assign retention and disposal classes
Significant information assets
Register in the organisations information asset register
Assign ownership and custodianship to the asset
Carry out risk assessment and assess for inclusion in WoVG information asset register
Develop quality statements if sharing or releasing
Manage strategically
Critical information assets
Develop quality statements
Create data quality management plans
Include in department business continuity plan
A weather agency creates/collects a range of information assets while fulfilling it's function – observing, recording and communicating weather information to the public
Purchase records for office stationery and stores
Procurement documentation for the acquisition of specialised observational equipment or infrastructure
Public weather warnings are created and issued and form part of the historical weather records of the country

**Figure 4 – Information assets**

- the information asset is valuable to the public
- the information asset belongs to an external entity and is managed by the department on behalf of an external information owner
- the information asset is used as input or output of a core business process or is fundamental to a key decision-making process i.e. without the information business continuity is severely compromised
- the information asset contributes significantly to corporate knowledge
- the information asset is received from an external department or source and exchanged on a regular basis
- the information asset is of high public value and its replacement is cost prohibitive or impossible.

All significant information assets must be registered in the department's information asset register.

## Critical information assets

**Critical information assets** are a subset of the identified significant information assets and are those assets that are considered high value/high risk or vital to the department. Loss, damage, destruction or lack of availability of a critical information asset would be disastrous to the organisation and affect essential operational functions[7].

Critical information assets must be identified as critical in the department's information asset register and should be included in organisational business continuity, strategic and project planning. Critical information assets must be managed with a level of control commensurate with their value and risk profile.

The CPDP's guidance *Stages of the Information Value Assessment Process* and *VPDSF Business Impact Level (BIL) Table* and PROV's guidance *What is high value, high risk?* are useful tools for determining how critical an information asset is.

As per Figure 4 – Information assets above, examples of critical and significant information assets include:

| Information Asset | Examples |
|---|---|
| All | • Purchase records for office stationery and stores<br>• A guideline on how to collect client information<br>• Newsletters to clients<br>• Paid invoices |
| Significant | • Procurement documentation for the acquisition of specialised observational equipment or infrastructure<br>• De-identified client information<br>• Contracts and memorandums of understanding<br>• Risk registers |
| Critical | • Public weather warnings are created and issued and form part of the historical weather records of the country<br>• Identifiable client information<br>• Financial data |

## Information asset registers

This standard requires the identification and registration of all significant and critical information assets in a departmental IAR in accordance with the metadata requirements outlined in the Information Asset Register Standard.[8]

Custodians should register assets once created or acquired. Departments may also wish to register planned assets to help identify duplication before any investment is made.

[7] 5. Vital records protection (Counter Disaster Strategies), NSW Government State Archives & Records, 2015 https://www.records.nsw.gov.au/recordkeeping/advice/counter-disaster-strategies/5-vital-records-protection

[8] The Information Asset Register Standard is flagged for development in 2017.

### WoVG information asset register

The government intends to develop a whole of Victorian Government (WoVG) IAR. The aim of this IAR will be to:

- increase discoverability and access to government information
- reduce duplication, create opportunity for data reuse, repurpose, integration and transformation
- facilitate the development of insight for decision making, policy development and service delivery.

The WoVG IAR will provide searchable metadata for information asset discovery with contact information to obtain data access.

## Information risk management

9. Incorporate operational and strategic information-related risks into enterprise, divisional, program and project risk management.

Identifying, evaluating and mitigating risks (threats, vulnerabilities and consequences) around information helps to protect its confidentiality, integrity and availability. It also helps to prioritise information and information management improvement activities.

Departments must incorporate information risks into the risk management framework of their organisation. Consideration should be given to both risks arising from information management activities and risks arising out of business activities which may be mitigated by better information management practice.

Consider using your department's risk management framework or the Victoria Government Risk Management Framework and the Victorian Management Insurance Agency's Victorian Risk Management Framework practice guide.

## Legislation and compliance

10. Manage information according to all relevant legislation (national, state and department specific) and policies, and ensure the department's audit and compliance program measures information management compliance.

### Legislation and administrative obligations

Departments must ensure they comply with all relevant legislation and administrative policies, in the creation, storage, management, use, sharing or release of information including:

- *Privacy and Data Protection Act 2014 (Vic)*
- *Freedom of Information Act 1982 (Cth)*
- *Public Records Act 1973 (Vic)*
- *Health Records Act 2001 (Vic)*
- *Evidence Act 2008 (Vic)*
- *Copyright Act 1968 (Cth)*

- *Financial Management and Accountability Act 1997 (Cth)*
- *DataVic Access Policy*
- *WoVG Intellectual Property Policy*

Departments must also determine if they are subject to any further legislation, regulations or policies etc. that impact the way their information is created, stored, managed, used, shared or released.

This requirement is about proactive and planned management of information in accordance with statutory and administrative obligations. A key role of the IMGC is to ensure activities within these areas are well coordinated.

Departments may utilise the IM GUIDE 05 Information Management checklist for systems procurement and implementation as a prompt.

## Audit and compliance

Each department is required under the Standing Directions of the Minister for Finance to have an internal audit function. The internal audit function should, periodically, audit against the WoVG Information Management Policy and associated policies and standards to assist departments in identifying deficiencies in information management practice.

Measuring progress levels again compliance requirements will also, over time, provide valuable insights on the effectiveness of information management initiatives and allow the department to identify areas of good practice and opportunities for improvement.

# Further information

For further information regarding this standard, please contact Enterprise Solutions, Department of Premier and Cabinet, at: enterprisesolutions@dpc.vic.gov.au.

# Appendix A: Sample IMGC terms of reference

## Introduction

This document contains the terms of reference for the 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 the Victorian Government's (government) Information Management Framework, Information Management Policy and associated standards
- building organisational capability and capacity in information management
- monitoring and reporting compliance with government and department information-related policies and standards
- monitoring and reporting compliance with statutory and administrative obligations
- ensuring coordination across information-related functions including privacy, freedom of information  and information security
- providing input into government information priorities via the Information Management Group, the CIO Leadership Group and related reference and working 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
- ensure that the IMGC meeting's objectives are fulfilled.

### Members

The IMGC includes the following functional representation:

- department CIO (or equivalent)

- chief information security officer (CISO)
- senior line-of-business representatives with critical 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
- be collectively accountable for the delivery of the department'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 department's information management works program.

## Meeting management

Decision-making process

When possible, decisions should be 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 and will be considered as having the same accountability as the nominal IMGC member.

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 department information management works program
- updates to government-wide information-related policies and standards
- information management compliance monitoring and reporting
- 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 department head (see Figure 6 - IMGC Governance Model).

It communicates with and provides advice and feedback, as required, to:

- the CIO Leadership Group
- the government's Information Management Group
- other department IMGCs (as required for networking and information sharing purposes).

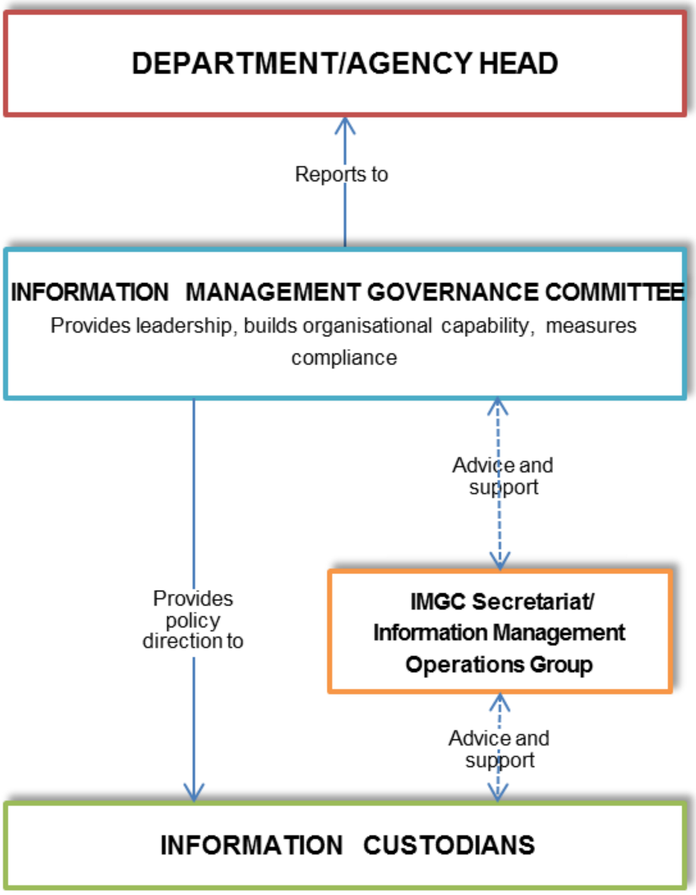

DEPARTMENT/AGENCY HEAD
Reports to
INFORMATION MANAGEMENT GOVERNANCE COMMITTEE
Provides leadership, builds organisational capability, measures compliance
Advice and support
Provides policy direction to
IMGC Secretariat/ Information Management Operations Group
Advice and support
INFORMATION CUSTODIANS

Figure 5 - IMGC Governance Model