



Information Management Maturity Measurement

Developing IM in Your Organisation

Version 1.7, December 2019

Copyright Statement

© State of Victoria 2019



Except for any logos, emblems, and trade marks, this work (IM3 Developing IM V1.7) is licensed under a Creative Commons Attribution 4.0 International license, to the extent that it is protected by copyright. Authorship of this work must be attributed to the Public Record Office Victoria. To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0/legalcode>.

Disclaimer

The State of Victoria gives no warranty that the information in this version is correct or complete, error free or contains no omissions. The State of Victoria shall not be liable for any loss howsoever caused whether due to negligence or otherwise arising from the use of this document.

Contents

INTRODUCTION	3
1. PEOPLE	4
1.1: Information Literacy and Responsibility	4
1.2: Capability and Capacity	5
1.3: Training, Support and Knowledge Sharing	6
2. ORGANISATION	8
2.1 Governance	8
2.2 IM Strategy and Vision.....	9
2.3 Strategic Alignment	11
2.4 Management Support and Leadership.....	13
2.5 Audit and Compliance	14
3. INFORMATION LIFECYCLE and QUALITY	16
3.1 Asset Management.....	16
3.2 Policies and Procedures.....	18
3.3 Meeting Business Needs.....	20
3.4 Accessibility and Discoverability.....	22
3.5 Information Use and Reuse	24
4. BUSINESS SYSTEMS and PROCESSES	26
4.1 Information Architecture.....	26
4.2 Process Improvement.....	27
4.3 Business Systems and Tools	28
4.4 Information Privacy and Security	30

INTRODUCTION

About This Document

This document provides information to assist with the use of the Public Record Office Victoria (PROV) Information Management Maturity Measurement (IM3) assessment tool. It contains information about each of the characteristics in the assessment, and includes:

- a description of each Information Management (IM) characteristic
- suggestions for developing your organisation's current level of maturity
- references to Victorian Government and other resources.

Assessing Overall Results

The IM3 results can be used to indicate an overall status of information management in your organisation. For example:

- If the majority of characteristics (e.g. 10 out of 17) were assessed at Level 2, this may indicate an overall underdeveloped program of IM initiatives.
- If the majority of characteristics were assessed at Level 3 or 4, you may want to consolidate practices at these levels by consulting the relevant standards and policies.

Examine your results to see if there are any patterns or trends that can inform your planning and actions. For example:

- Are the results strong in one dimension but weak in other? For example, are the PEOPLE characteristics well developed, but all ORGANISATION characteristics underdeveloped?
- Do the results point to an issue in a particular business function? For example, are all operational characteristics underdeveloped but strategic characteristics strong?
- Do the less mature characteristics fall under the responsibility of a single area of the business or many? Do you have influence or control of these characteristics?
- Are there dependencies between the characteristics that you can identify? For example, the 'Accessibility and Discovery' characteristic is underdeveloped because it is dependent on developing 'Business Systems and Tools'.

1. PEOPLE

1.1: Information Literacy and Responsibility

Are staff in your organisation aware of their IM responsibilities?
Is information regarded and treated as a valuable asset?

About this Characteristic

Information literacy is the the ability to know when there is a need for information. An example of this would be the ability for staff members of an organisation to identify, locate, evaluate, and effectively use information to address specific issues or challenges.

Responsibility for information includes ensuring that people are aware of:

- the organisation’s information needs
- the role and value of information as assets in the organisation
- the skills and knowledge required to use and manage information responsibly and effectively.

Examples of Information Literacy

Examples of evidence supporting information literacy include the following:

- Staff are aware of the importance of information and data management to the organisation and of their responsibilities in relation to it.
- Staff are educated and encouraged to exploit information and data to the fullest. They actively engage in new IM initiatives and seek better understanding of the organisation’s information assets.
- Staff IM and data management responsibilities are defined in documentation such as policies, processes and job descriptions.
- IM training is provided during staff on-boarding/orientation.
- IM and data management training programs are in place in the organisation and are reviewed and updated as required.

Victorian Government Resources

Resource	Link
<i>Information Management Policy for the Victorian Public Service</i> , Enterprise Solutions (ES)	https://www.enterprisesolutions.vic.gov.au/information-management/

1.2: Capability and Capacity

Is the organisation's capability and capacity sufficient to support and develop good information management?

About this Characteristic

Capability is a feature, faculty or process that can be developed or improved as well as the individual skills that can be applied to do this. Capability answers the questions:

- *How can we improve our practices?*
- *What competencies do current staff have that can be applied and exploited?*
- *How easy is it to access, deploy or apply any additional capability?*
- *How much IM capability is needed in the organisation?*

Capacity is the power to hold, receive or accommodate and addresses the 'amount' or 'volume' concerned. Capacity answers the questions:

- *Do we have enough skills/knowledge/process/policies?*
- *How much is needed?*
- *Are there key areas of the business where IM capacity should be extended?*
- *Will more be needed in the future?¹*

Examples of IM Capability and Capacity

Examples of evidence supporting IM capability and capacity include the following:

- Strategies and/or programs of work have been implemented to address any gaps in IM and data management skills, capability and capacity.
- The organisation gives priority to recruiting specialists to help develop the organisation's IM and data management capability.
- The human resource requirements for IM and data management are regularly assessed in terms of capacity, skills and knowledge.
- IM and data specialists are respected professionals who are consulted in the development and implementation of business initiatives.
- IM and data specialists have been appointed into dedicated roles.
- There are a sufficient number of staff employed in IM roles in the organisation.
- IM projects and initiatives are adequately resourced and funded within the organisation.

Victorian Government Resources

Resource	Link
<i>Information Management Framework</i> , ES	https://www.enterprisesolutions.vic.gov.au/information-management/

Other Resources

Resource	Link
<i>Information Management Specialist</i> , Queensland Government CIO	https://www.qgcio.qld.gov.au/information-on/workforce-planning/ict-career-streams/information-management-specialist

¹ Vincent, L. 2008, 'Differentiating competence, capability and capacity', *Innovating Perspectives*, vol. 16, no. 3, <<http://www.innovationthatwork.com/images/pdf/June08newsltr.pdf>>.

1.3: Training, Support and Knowledge Sharing

What training, support or knowledge sharing is available to staff in your organisation to assist them in meeting their IM responsibilities?

About this Characteristic

Training in IM encompasses a wide range of skills and knowledge, including:

- knowledge of relevant legislation and standards
- general information, data and records management principles and practice
- the ability to analyse business processes
- effective communication skills
- management of information, data and records management projects
- understanding the digital capabilities of business systems used across the organisation.

Your organisation should ensure all staff are trained to understand their information, data and records management responsibilities. This includes:

- senior management
- ongoing and non-ongoing staff
- full-time and part-time staff
- contract and volunteer staff.

Examples of IM Training, Support and Knowledge Sharing

Examples of evidence supporting IM training, support and knowledge sharing include the following:

- The organisation has established initiatives to help build the IM culture, foster positive attitudes to IM and educate staff on their IM responsibilities.
- Staff have access to a range of internal or external IM, data management and records management courses and/or knowledge sharing tools relevant to their job role.
- Training is regularly reviewed and updated to suit needs.
- Formal training has been established and is regularly maintained to build practical skills and knowledge.
- Staff are in place to deliver and maintain quality training.
- Documentation/tools such as contact information, manuals and reference guides are available to staff.

1.3: Training, Support and Knowledge Sharing, continued

Victorian Government Resources

Resource	Link
<i>Recordkeeping Essentials</i> (online course - forthcoming), PROV	https://www.prov.vic.gov.au/recordkeeping-government/learning-resources-tools/online-recordkeeping-training
<i>PROS 19/04 Operational Management Standard</i> , PROV	https://prov.vic.gov.au/recordkeeping-government/document-library/pros-1904-operational-management-standard

Other Resources

Resource	Link
<i>Support and professional development</i> , National Archives of Australia (NAA)	https://www.naa.gov.au/information-management/support-and-professional-development
<i>Education and Training</i> , Records and Information Management Professionals Australia (RIMPA)	https://www.rimpa.com.au/events/education-and-training/

2. ORGANISATION

2.1 Governance

To what degree is IM formally governed in your organisation?

About this Characteristic

Central governance within organisations is needed to ensure coordination, visibility and appropriate sponsorship of IM activities.

Minimum requirements for IM governance are set out in *IM STD 03 Information Management Governance Standard* developed by Enterprise Solutions (ES). This includes the establishment and maintenance of an internal Information Management Governance Committee (IMGC), or similar to lead, monitor and report on information management activities. It also includes biannual participation in IMMAP.

Examples of IM Governance

Examples of evidence supporting IM governance include the following:

- An internal governing body (IMGC) has been established to lead, monitor and report on IM activities.
- The IMGC ensures coordination, visibility and appropriate sponsorship of information management activities within the organisation.
- The IMGC is chaired by an executive-level officer, reports to the department head (or a peak executive body chaired by the department head) and has representation from key business areas of the organisation.
- The organisation head supports and values the work of the IMGC.

Victorian Government Resources

Resource	Link
<i>IM STD 03 Information Management Governance Standard</i> , ES	https://www.enterprisesolutions.vic.gov.au/information-management/
<i>IM GUIDE 06 Information Management Governance Guide</i> , ES	https://www.enterprisesolutions.vic.gov.au/information-management/
<i>PROS 19/03 Strategic Management Standard</i> , PROV	https://prov.vic.gov.au/recordkeeping-government/document-library/pros-1903-strategic-management-standard
<i>Victorian Protective Data Security Standards</i> , Office of the Victorian Information Commissioner (OVIC)	https://ovic.vic.gov.au/data-protection/standards/

Other Resources

Resource	Link
<i>Information governance</i> , NAA	http://www.naa.gov.au/information-management/information-governance/
<i>Best practices in implementing an information governance policy</i> , (podcast, 15 mins), Jonathan Gourlay, Techtarget	http://searchcontentmanagement.techtarget.com/podcast/Best-practices-in-implementing-an-information-governance-policy

2.2 IM Strategy and Vision

Does the organisation have a strategy that provides a roadmap for IM?
Has the organisation formulated and articulated its vision for IM?

About this Characteristic

An IM strategy is an organisation's vision for its information management and the systematic approach to achieving this vision. It acknowledges the extent to which a modern organisation depends on information, and considers how this valuable asset should be managed.

"A culture of information management is one that recognizes the strategic value of information to the institution and promotes and facilitates good information management practice."²

Legislation

Legislation specific to your organisation or its business will need to be reflected in your information management strategy. At a minimum, this should include:

- *Public Records Act 1973*
- *Privacy and Data Protection Act 2014*
- *Health Records Act 2001*
- *Data Sharing Act 2017.*

Examples of IM Vision and Strategy

Examples of evidence supporting information management vision and strategy include the following:

- An IM strategy has been developed, implemented and endorsed to outline the organisation's vision for the systematic approach to the management of information and data.
- Other strategic documents are in place in the organisation, which adequately cover IM needs and initiatives.
- The strategy adequately highlights organisation-wide IM issues, major risks, desired results and the resource implications.
- Strategy development was achieved through collaboration between IM and business representatives to align to the organisation's vision, strategic objectives and business drivers.
- The IM strategy is assessed for improvement on an annual basis. The initiatives of the IM strategy are resourced and funded.

² Hanson, T. 2011, *Making the Case for the Information Strategy: ECAR Research Bulletin 12, 2011*, EDUCAUSE Center for Applied Research, Boulder, Colorado.

2.2: IM Strategy and Vision, continued

Victorian Government Resources

Resource	Link
<i>Information Technology Strategy</i> , ES	https://www.vic.gov.au/information-technology-strategy
<i>Digital Workplace Strategy</i> , ES	https://www.vic.gov.au/digital-workplace-strategy
<i>PROS 19/03 Strategic Management Standard</i> , PROV	https://prov.vic.gov.au/recordkeeping-government/document-library/pros-1903-strategic-management-standard
<i>PROS 19/03 G Strategic Management Guideline</i> , PROV	https://prov.vic.gov.au/recordkeeping-government/document-library/pros-1903-g-strategic-management-guideline

Other Resources

Resource	Link
<i>Making the Case for the Information Strategy</i> , Terry Hanson, EDUCAUSE	http://www.educause.edu/library/resources/making-case-information-strategy
<i>Guidelines for Developing an Information Management Strategy</i> , Coopers and Lybrand and the JISC's Information Strategies Steering Group	http://web.archive.org/web/19980125112630/www.jisc.ac.uk/pub/infstrat/
<i>Recordkeeping including the Management of Electronic Records</i> , Audit Report No. 6, 2006–07, Australian National Audit Office (ANAO)	https://www.anao.gov.au/work/performance-audit/recordkeeping-including-management-electronic-records
<i>Information management strategy</i> , NAA	https://www.naa.gov.au/information-management/information-governance/establishing-information-governance-framework/developing-information-management-strategy
<i>8 Factors to Consider When Creating an Information Management Strategy</i> , AIIM ([American] Association for Information and Image Management)	http://www.aiim.org/pdfdocuments/40480.pdf

2.3 Strategic Alignment

To what degree is the IM strategy aligned with and incorporated into other strategic planning in your organisation?

About this Characteristic

The requirements and objectives in the IM strategy must align with the organisation's other management systems and business strategies. For example:

- information technology (IT)
- security
- risk
- occupational health and safety
- records management
- freedom of information (FOI)
- privacy
- environmental management.

Relationship of IT and IM Strategies

The relationship between an organisation's IM strategy and IT strategy can be confusing as they address many of the same areas. The following quote suggests the relationship of these two strategies:

*"The concept of an IT strategy cannot be divorced from the broader notion of an information strategy. The former is a necessary component of the latter...It follows that the IT strategy should be designed to facilitate the objectives and requirements of the information strategy...then this would suggest that the [IM strategy] stands as the relatively fixed statement of principles, whilst the [IT strategy] would be somewhat more nimble as it responds to circumstances and opportunities. The IT strategy, then, might take the form of a rolling program covering no more than three years, based on the broader strategic principles, managed and monitored...through the governance machinery."*³

Examples of Strategic Alignment

Examples of evidence supporting strategic alignment includes the following:

- IM obligations are identified and acknowledged in other key organisation policies.
- The IM strategy is aligned with and/or integrated with other strategic planning in the organisation (e.g. risk, privacy, FOI, IT, procurement, or environmental management strategies).
- IM capabilities are built into the business through strategy, policy and projects.
- New organisation projects and initiatives identify IM implications, dependencies and synergies.

³ Hanson, T. 2011, *Making the Case for the Information Strategy: ECAR Research Bulletin 12, 2011*, EDUCAUSE Center for Applied Research, Boulder, Colorado, p. 10.

2.3 Strategic Alignment, continued

Victorian Government Resources

Resource	Link
<i>Victorian Government Cyber Security Strategy 2016-2020</i> , Department of Premier and Cabinet (DPC)	https://www.vic.gov.au/victorian-government-cyber-security-strategy
<i>Victorian Protective Data Security Standards</i> , OVIC	https://ovic.vic.gov.au/data-protection/standards/
<i>PROS 19/03 Strategic Management Standard</i> , PROV	https://prov.vic.gov.au/recordkeeping-government/document-library/pros-1903-strategic-management-standard
<i>PROS 19/03 G Strategic Management Guideline</i> , PROV	https://prov.vic.gov.au/recordkeeping-government/document-library/pros-1903-g-strategic-management-guideline

Other Resources

Resource	Link
<i>Making the Case for the Information Strategy</i> , Terry Hanson, EDUCAUSE	http://www.educause.edu/library/resources/making-case-information-strategy

2.4 Management Support and Leadership

Does management support IM in your organisation?
Is there executive-level representation for IM initiatives?

About this Characteristic

The success of an organisation's IM strategy and practice relies upon the support of all levels of management and strong overall leadership and advocacy. This includes ensuring the link is made between IM capabilities and wider strategic objectives. The IMGC has an important role in ensuring executive sponsorship of information management across the organisation.

Ownership and leadership needs to be clear within and across organisations to ensure that significant risks associated with knowledge and information mismanagement are minimised. Questions to consider include the following:

- Does senior management actively support IM policies and practices?
- Do middle managers actively encourage staff to comply with IM policies and practices?
- Has a robust IM culture been instilled into your organisation?
- Have sufficient funding and other resources been allocated for IM?⁴

Examples of Management Support and Leadership

Examples of management support and leadership in IM include the following:

- The organisation has appointed an executive level Chief Information Officer (CIO), Chief Data Officer (CDO), or equivalent.
- IM interests and issues are represented at executive level and are given appropriate consideration.
- IM policies and practices are actively supported by senior management and middle management.
- Leadership understands IM issues and practices and seek additional specialist information when needed.

Victorian Government Resources

Resource	Link
<i>PROS 19/03 Strategic Management Standard</i> , PROV	https://prov.vic.gov.au/recordkeeping-government/document-library/pros-1903-strategic-management-standard
<i>PROS 19/03 G Strategic Management Guideline</i> , PROV	https://prov.vic.gov.au/recordkeeping-government/document-library/pros-1903-g-strategic-management-guideline

Other Resources

Resource	Link
<i>Recordkeeping including the Management of Electronic Records</i> , Audit Report No. 6, 2006–07, ANAO	https://www.anao.gov.au/work/performance-audit/recordkeeping-including-management-electronic-records

⁴ See 'Recommendation 3' in, Australian National Audit Office, 2003, *Recordkeeping in Large Commonwealth Organisations*, Canberra, ACT.

2.5 Audit and Compliance

How well does your organisation monitor compliance with your own IM standards and with Victorian Government mandated legislation and requirements?

About this Characteristic

This characteristic addresses both:

- how your organisation complies with IM requirements outlined in legislation, standards, policies and procedures
- to what degree staff perform tasks in accordance with these requirements.

Compliance must be monitored to ensure that information is created and effectively managed. Regular audits can identify gaps or problems and help to develop strategies to address these issues. All audits and reviews of organisation functions and activities should include an assessment of the compliance with legislation, standards and its own IM policies and procedures.

Assessing Compliance

To assess your organisation's compliance look for:

- established monitoring and compliance programs
- benchmarks for quantitative and qualitative measurement
- reporting arrangements
- evidence of follow-up action.

Management have a key role in ensuring that all staff are aware of their responsibilities, trained appropriately and carry out their duties accordingly.

Examples of Audit and Compliance

Examples of audit and compliance for IM include the following:

- The organisation has an internal audit process/program in place to work towards achieving compliance against IM-relevant legislation, policies and standards (such as those issued by PROV and OVIC).
- IM compliance requirements are known, communicated and applied within the organisation.
- Corrective actions have been implemented to address causes of non-compliance.
- Opportunities to improve IM compliance are explored and implemented.

2.5 Audit and Compliance, continued

Victorian Government Resources

Resource	Link
<i>Information Management Framework</i> , ES	https://www.enterprisesolutions.vic.gov.au/information-management/
<i>Records Management Checklist</i> (to audit your recordkeeping practices against PROV standards), Victorian Auditor-General's Office (VAGO)	https://www.audit.vic.gov.au/records-management-checklist
<i>PROS 19/04 Operational Management Standard</i> , PROV	https://prov.vic.gov.au/recordkeeping-government/document-library/pros-1904-operational-management-standard

Other Resources

Resource	Link
<i>Australian Standard Records Management</i> , AS ISO 15489.1, 2017, Standards Australia	Available from Standards Australia: https://www.standards.org.au/
<i>Monitoring recordkeeping performance</i> , State Archives and Records NSW	https://www.records.nsw.gov.au/recordkeeping/advice/monitoring/recordkeeping-performance

3. INFORMATION LIFECYCLE and QUALITY

3.1 Asset Management

How well does the organisation identify, manage and monitor their significant information assets?
Have IM roles and responsibilities been defined in the organisation to properly manage information assets?

About this Characteristic

Information assets are critical to decision-making and service delivery. Like other assets, information needs to be managed, maintained and have its value maximised. This can be achieved through a custodianship program which:

- clearly assigns and records responsibilities
- educates staff on their responsibilities
- identifies high value and high risk information assets.

Information Assets

A 'significant information asset' is a discrete collection of data or information that is recognised as valuable to the organisation. The following provides some examples of what to consider when assessing value:

- 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
- 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 source and exchanged on a regular basis
- the information asset is of high public value and its replacement is cost prohibitive or impossible.

Examples of information asset management

Examples of information asset management include the following:

- The organisation's significant information assets (i.e. discrete collections of data or information that is recognised as valuable to the organisation) and critical information assets (i.e. subsets of significant information assets that are considered high value/high risk or vital to the organisation) have been identified.
- An information asset register (IAR) has been established and maintained to document at minimum, the organisation's significant information assets.
- A custodianship model is in place so that assets have an assigned owner and custodian.
- The custodianship model supports work with information users to actively maintain assets and improve the accessibility, usability and sharing of information as required.
- Users can assess if assets are fit for their intended purpose.

3.1 Asset Management, continued

Victorian Government Resources

Resource	Link
<i>IM STD 03 Information Management Governance Standard</i> , ES	https://www.enterprisesolutions.vic.gov.au/information-management/
<i>IM GUIDE 06 Information Management Governance Guide</i> , ES	https://www.enterprisesolutions.vic.gov.au/information-management/
<i>Practitioner Guide Identifying and Managing Information Assets v2.0</i> , OVIC	https://ovic.vic.gov.au/resource/practitioner-guide-identifying-and-managing-information-assets-v2-0/
<i>PROS 19/03 Strategic Management Standard</i> , PROV	https://prov.vic.gov.au/recordkeeping-government/document-library/pros-1903-strategic-management-standard
<i>PROS 19/03 G Strategic Management Guideline</i> , PROV	https://prov.vic.gov.au/recordkeeping-government/document-library/pros-1903-g-strategic-management-guideline

Other Resources

Resource	Link
<i>Information assets and their classification guideline</i> , Queensland Government Chief Information Office	https://www.qgcio.qld.gov.au/documents/information-assets-and-their-classification
<i>Information asset register guideline</i> , Queensland Government Chief Information Office	https://www.qgcio.qld.gov.au/documents/information-asset-register-guideline

3.2 Policies and Procedures

Does the organisation have fully developed and implemented IM policies that align to relevant legislation and standards?

Are these policies supported by documented procedures?

About this Characteristic

DPC, PROV and OVIC have developed standards for IM, records management, information access, privacy, security and intellectual property. Organisations should develop their own policies and procedures to inform staff how to practically implement those standards. The policies and procedures will provide the basis for staff to create and manage authentic, reliable and usable information for business and accountability purposes.

Note that:

- A *strategy* defines the overall character, mission and direction of an organization. The focus of a strategy is on an organisation's long-term relationship with its external environment, and specifies what an organisation will be doing in future. Strategies are formulated and implemented with a view to achieve specific goals.
- A *policy* tells people what they should and should not do in order to contribute to the achievement of corporate goals. It explains how goals will be attained and makes the strategy of the business explicit. Specific procedures are then derived from policies.⁵ A *policy* is a concise document that identifies responsibilities and rules.
- A *procedure* provides step-by-step details regarding how to do something in accordance with the rules.

Characteristics of an Effective Policy

An effective information and records management policy will:

- align with the organisation's environment, strategic direction, policy framework, and IM programme
- reflect current business and legislative needs
- be endorsed and actively supported and resourced by the senior executive
- be implemented and communicated regularly across the whole organisation
- cover all systems that contain information
- cover all practices associated with information
- be linked to related business policies and programmes
- be supported by sets of procedures, guidance, and tools
- enable compliance assessment to be monitored
- be assessed regularly.

Evidence of Policies and Procedures

Evidence of IM policies and procedures include the following:

- The organisation has established IM policies that align to relevant legislation and standards (such as those issued by PROV and OVIC).
- The policies have been approved and endorsed by the Secretary or an executive level board/officer. The policies are actively communicated and available to all staff.
- IM procedures have been established and implemented within the organisation.
- Policy and procedures are appropriate to the organisation's business and are reviewed for improvement as required.
- Breaches of policy are actively addressed and rectified.

⁵ Citeman, 2010, *Strategy versus Policy*, < <https://www.citeman.com/11817-strategy-versus-policy.html>>.

3.2 Policies and Procedures, continued

Victorian Government Resources

Resource	Link
<i>Information Management Policy</i> , ES	https://www.enterprisesolutions.vic.gov.au/information-management/
<i>PROS 19/03 G Strategic Management Guideline</i> , PROV	https://prov.vic.gov.au/recordkeeping-government/document-library/pros-1903-g-strategic-management-guideline

Other Resources

Resource	Link
<i>Australian Standard Records Management</i> , AS ISO 15489.1, 2017, Standards Australia	Available from Standards Australia: https://www.standards.org.au/
<i>Information management policy</i> , NAA	https://www.naa.gov.au/information-management/information-governance/establishing-information-governance-framework/developing-information-management-policy

3.3 Meeting Business Needs

Is information meeting the needs of the business and its users in terms of strategic importance, quality and availability?

About this Characteristic

One of the five key IM principles is that 'Information is fit for its intended purposes and is easy to find, access and use'⁶. The rationale for this principle is that the way that information is created and managed is based on its operational and strategic importance, its risk profile, and the needs of all its users - citizens, government, partner organisations and industry.

Information Needs Analysis

To ensure that staff have access to information that meets their needs now and in the future, an information needs analysis can be conducted. This will provide you with a framework with which you can more pro-actively plan for the future. An information needs analysis aims to answer two main questions:

- What information do we have now?
- What information do we want to have?

The shortfall between these two questions will provide you with the necessary direction to focus your energies.

Risks of Not Meeting Needs

Risks and symptoms of not meeting information needs appropriately may include:

- difficulty for staff to obtain a single and comprehensive source of information.
- evidence of a misalignment between strategic business direction and systems architecture.
- difficulties for staff in searching for and identifying information.
- staff not being aware of available information resources.
- the proliferation of processing systems, local systems and fragmented information stores.

Evidence of Meeting Business and User Needs

Evidence of meeting business and user needs regarding IM includes the following:

- The organisation has established processes and/or a program to address information quality issues (ensuring information is accurate, consistent, complete and current).
- An analysis of information assets has been conducted to determine if information is meeting business needs, accountability requirements and community expectations.
- Data quality statements have been developed for at least the significant (including critical) information assets.
- Remediation processes are in place to address information (and data) quality and/or availability issues.
- On the whole, information is fit for purpose and/or can be tailored to meet business needs.

⁶ Enterprise Solutions, 2018, *Information Management Policy for the Victorian Public Service*, Melbourne, <<https://www.enterprisesolutions.vic.gov.au/wp-content/uploads/2017/08/POL-IM-01-Information-Management-Policy.pdf>>.

3.3 Meeting Business Needs, continued

Victorian Government Resources

Resource	Link
Victorian Centre for Data Insights (VCDI)	https://www.vic.gov.au/datainsights.html
<i>Policy and Standards</i> (including Access and IP Policies), DataVic	https://data.vic.gov.au/datavic-access-policy
<i>Information Management Policy</i> , ES	https://www.enterprisesolutions.vic.gov.au/information-management/

3.4 Accessibility and Discoverability

How easy is it for organisation staff and other parties to find the information they are looking for?
Is critical information able to be found in a timely manner when it is needed?

About this Characteristic

The public, government employees and partner organisations must be able to find the information they need when they need it to function efficiently. To find and use information it must be both discoverable and accessible.

For information to be discoverable it must be easily found and/or navigated. This involves concepts such as the following:

- Metadata – making information easier to find by applying appropriate metadata.
- Security and Privacy – restricting access to some information due to security, privacy, confidentiality or commercial risks.
- Collaboration - organisations working towards a common cross-government information directory and other mechanisms for facilitating information discovery.

Note that while search technology is an important component of an overall information environment, it is not a substitute for good information management cultures and processes.

For information to be accessible it must be readable and useable. This includes concepts such as:

- interoperability
- multilingualism
- open source software
- open content
- Creative Commons licences
- addressing the special needs of people with disabilities.

Evidence of Information Accessibility and Discoverability

Examples of evidence supporting information accessibility and discoverability include the following:

- An organisation-specific information repository and/or search applications have been developed and are used by staff.
- Information is collected and stored with access and discoverability in mind.
- Definitions and standards are used to increase the findability of information.
- Sufficient metadata is provided to correctly identify and locate information.
- Access to controlled information sources has been defined and implemented.
- Procedures have been implemented for information capture, the application of metadata, information access, storage and retrieval.

3.4 Accessibility and Discoverability, continued

Victorian Government Resources

Resource	Link
<i>Information Management Policy</i> , ES	https://www.enterprisesolutions.vic.gov.au/information-management/
<i>Victorian Government Data Directory</i> , DataVic	https://www.data.vic.gov.au/
<i>Make content accessible</i> (Digital Standards how-to guide), DPC	https://www.vic.gov.au/digitalstandards/design-build/make-content-accessible.html

Other Resources

Resource	Link
<i>Build the business case for an enterprise search platform</i> , (podcast, 15 mins), Jonathan Gourlay, TechTarget	http://tinyurl.com/accbbfk
<i>Information Accessibility</i> , UNESCO, Information for all Programme (IFAP)	http://www.unesco.org/new/en/communication-and-information/intergovernmental-programmes/information-for-all-programme-ifap/priorities/information-accessibility/

3.5 Information Use and Reuse

How usable is the information being produced by the organisation, both now and in the future?

About this Characteristic

- Information 'usability' addresses how information is collected, organised, described, presented defined and shared. The term 'usability' is often used in relation to web sites and user interface design, but can apply to any information source.
- Information 'reuse' addresses the concept of 'Interoperability', which is the ability of organisations to share data and information by the use of common standards, licences and open data.

Encouraging Usability

The following questions may be helpful when assessing the usability of digital information sources and systems:

- Is the structure and organisation of the document, system or site clear to a user?
- Is there a site map, contents, index, search function or other finding aid?
- Does the structure of the information support the purpose of the information?
- Does the user have the freedom to control or filter the information they see?
- Is there the ability to undo a mistake?
- Can users exit the system or information when they choose to, or are they locked into a specific path?
- Is language clear, simple and appropriate to the audience?
- Does the language follow real-world conventions, making information appear in a natural and logical order?
- Is there a feedback or help function available?
- Is the layout and design of the site/page consistent?
- Is terminology used consistently?
- Can users predict the content of a page or screen by its title?
- Is the layout of information clear, uncrowded and pleasing to the eye?
- Are labelling, sub-headings or tables used to provide better access to information?

Information Reuse

Victorian government encourages the reuse of information through various means, including legislation (such as the *Victorian Data Sharing Act 2017*) and the Victorian government Data Directory (also known as data.vic.gov.au).

The *Victorian Data Sharing Act 2017* was developed to enable data sharing across government and address key priorities in the community. The Act provides a clear legal framework for sharing and using data across government, while providing strong safeguards and oversight. Under the Act, the Chief Data Officer (CDO) was appointed to lead the Victorian Centre for Data Insights (VCDI) and advocate for the better use of data across government. Sharing and using data across government improves policy making, service planning and design.

Organisations should refer to the VCDI's guidance materials as well as IM framework content related to data management (DM) and information sharing and release. Organisations are also encouraged to share their data with the public via data.vic.gov.au. This is a specialised website that helps members of the public find datasets and data tools that exist on government websites.

3.5 Information Use and Reuse, continued

Evidence of Information Use and Reuse

Examples of evidence supporting information use and reuse include the following:

- Organisation standards/procedures have been introduced to facilitate consistent information collection, description and organisation, and to prevent information duplication.
- Digital continuity strategies are in place. Information assets are shared and re-used across the organisation and with external stakeholders as appropriate.
- The organisation applies appropriate licences and quality statements when sharing information.
- Where appropriate, information is released to the public.
- Custodians work with information users to support the usability of information.
- The organisation is able to leverage their information for business intelligence and analytics.
- Data exchanges occur using standard interfaces and formats.

Victorian Government Resources

Resource	Link
Victorian Centre for Data Insights (VCDI)	https://www.vic.gov.au/datainsights.html
Victorian Government Data Directory, DataVic	www.data.vic.gov.au
Policy and Standards (including Access and IP Policies), DataVic	https://data.vic.gov.au/datavic-access-policy

4. BUSINESS SYSTEMS and PROCESSES

4.1 Information Architecture

Has the organisation developed an Information Architecture model?
To what degree does it link to other relevant models?

About this Characteristic

Information architecture (IA) refers to the design, arrangement and layout of an organisation’s information and the inter-relationships of information systems. An IA plan or document outlines how an organisation’s information and records must be described and organised. This makes it easier for information to be delivered in the correct context to the correct people.

To ensure a high level of adoption throughout the organisation, the IA should:

- be enterprise-wide in its scope
- have high-level endorsement for its intent, application and evolution
- promote flexible, standards-based information sharing and re-use
- be intrinsic to governance decisions for new system initiatives and business process change management.⁷

Relationship to Enterprise Architecture

In a mature organisation, there will be a close and coordinated relationship between the IA and the other strategies that make up the organisation’s enterprise architecture. This may include the:

- business architecture, which articulates the functional structure of an enterprise in terms of its business services and business information
- information technology architecture, which is a blueprint of how an organization’s IT and information management elements work together to efficiently accomplish the mission of the organization, including business activities, processes, data sets, information flows, applications and software.

Evidence of IA

Examples of evidence supporting IA includes the following:

- The organisation has developed an IA model which provides an overview and description of the organisation's information and its relationships to:
 - business requirements, systems and processes
 - applications and technology, and
 - strategies, standards and legislation.
- The model is managed and resourced and maintained accordingly.
- The IA aligns to other models such as the IT and Data Architectures.

Other Resources

Resource	Link
The Information Architecture Institute (based in USA)	http://www.iainstitute.org/

⁷ National Archives of Australia, 2010, *Check-up 2.0*, Commonwealth of Australia, Canberra.

4.2 Process Improvement

How well have business processes been aligned with IM requirements?

Has the organisation identified areas for improvement and eliminated duplicate processes?

About this Characteristic

Business process improvement is a systematic approach to help an organisation optimise its underlying processes to achieve more efficient results. In regard to IM, process improvement can be used to:

- identify the sources and flow of information in the organisation
- identify and eliminate information duplication
- define the logical arrangement and grouping of information
- define business contextual links between information
- implement preventative or corrective actions.

Business Process Management and Data Governance

Business process management can also benefit the information governance program. For example:

- *Data at the source* – The intelligent use of business process tools can help data custodians to reach back into upstream processes to fix data quality issues at the point of creation.
- *Data custodian efforts* – The data governance program will have a higher probability of success if it focuses on a high-impact business process and a handful of critical attributes.
- *Value of data governance to the business* – The business may say that IT owns the data, but they will never say that IT owns the business process. So starting from the business process is a good way to engage business users around data governance.

Evidence of Process Improvement

Examples of evidence supporting process improvement for IM includes the following:

- IM practices have been incorporated into business processes.
- Efforts have been made to look at where business processes can be re-engineered to improve efficiencies and reduce duplication of information and data.
- Process issues impacting IM are directed to appropriate staff or working groups for action.
- Process owners are open to making changes to improve process and IM outcomes and develop/update process documentation accordingly.

Other Resources

Resource	Link
<i>Standard Information and documentation – Work process analysis for recordkeeping, SA/SNZ TR ISO 26122:2012, Standards Australia</i>	Available from SAI Global: https://infostore.saiglobal.com/
<i>How to Map Data Governance Policies to Business Processes, Sunil Soares 2012, Information Management.com</i>	http://www.information-management.com/news/how-to-map-data-governance-policies-to-business-processes-10023600-1.html

4.3 Business Systems and Tools

Are IM capabilities built into business systems and tools?

About This Characteristic

In line with the technology reform area of the Victorian government's *Information Technology Strategy 2016 to 2020*, ES at DPC has developed *Statements of Direction* to guide future procurement and provide a common view on high-level requirements for government enterprise systems such as human resources, finance and briefing systems.

What is a Business Information System?

A business information system is any system that assists an organisation to perform its business and manage information. Examples include case management systems, staff management, pay systems, and finance systems. In supporting your organisation's business, systems that manage information need to work so that records:

- can be proven to be genuine
- are complete, accurate and can be trusted
- are secure from unauthorised access, alteration and deletion
- are findable and readable, and
- are related to other relevant records.

To achieve these characteristics, business information systems designers, owners and managers must take a systematic and consistent approach, by identifying IM requirements for their current and future systems.

Information is likely to be held in a number of different systems, but should not exist in unmanaged environments where oversight is limited or impossible.

Organisations should plan for technology variables that might be needed to support its information assets in the future (for example, changing access requirements, the addition or removal of information and the impact of new or amended policy).

Evidence of Business Systems and Tools

Examples of evidence supporting business systems and tools for IM includes the following:

- IM specialists works together with IT, RM and DM specialists as required to manage existing and/or implement new systems and tools.
- Information managed within the organisation's business systems and tools is effectively managed according to requirements from DPC, PROV and OVIC.
- The organisation encourages and adopts improvements to system and tool IM capabilities.
- Systems and tools are effectively managed over their life, from acquisition to decommissioning, to ensure their integrity, reliability and performance.

4.3 Business Systems and Tools, continued

Victorian Government Resources

Resource	Link
<i>PROS 19/04 Operations Management Standard, PROV</i>	https://prov.vic.gov.au/recordkeeping-government/document-library/pros-1904-operational-management-standard
<i>Statements of Direction, ES</i>	https://www.vic.gov.au/enterprise-systems-statements-direction
<i>Business systems, policies and standards, ES</i>	https://www.enterprisesolutions.vic.gov.au/business-systems-policy-and-standards/
<i>Information Technology Strategy 2016 to 2020, ES</i>	https://www.enterprisesolutions.vic.gov.au/strategies/information-technology-strategy/

Other Resources

Resource	Link
<i>ISO 16175 - what you need to know, NAA</i>	https://www.naa.gov.au/information-management/information-management-standards/iso-16175-what-you-need-know
<i>Checklist for assessing business systems, State Archives and Records NSW</i>	https://www.records.nsw.gov.au/recordkeeping/advice/checklist-for-assessing-business-systems

4.4 Information Privacy and Security

What is the status of information privacy and security in the organisation?

Do staff have the knowledge and support to protect information and ensure its confidentiality, integrity and availability?

Is the organisation able to respond to information privacy and security incidents?

About this Characteristic

The secure management of information is critical to government service delivery, public trust and confidence. Various legal, regulatory and administrative requirements govern the protection of official information designed to reduce information security risks and maintain individual's privacy (i.e. *Privacy and Data Protection Act 2014*, *Health Records Act 2001* etc.).

Each agency or body operates under a variety of legal, regulatory and administrative requirements, governing the protection of the information the organisation accesses, uses and holds.

Information Privacy

Information privacy protections are embodied in ten Information Privacy Principles (IPPs) set out in Schedule 1 of the *Privacy and Data Protection Act 2014* (PDP Act). The IPPs set out the minimum requirements for how personal information is to be collected and handled by public sector organisations. Under the Section 3 of the PDP Act:

'personal information' means information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the Health Records Act 2001 applies.

Protective Data Security (Information Security)

Protecting information (including personal information) is the practice of applying *risk-based controls*, commensurate with the *value* of an organisation's *information assets*. Selected security measures are used by organisations to ensure the continued **confidentiality**, **integrity** and **availability** of their official information.

The PDP Act provides for the Victorian Protective Data Security Framework (VPDSF) which, with limited exceptions, applies to the majority of Victorian public-sector agencies or bodies. It has been developed to help organisations:

- identify information assets
- assess the value of this information
- identify and manage protective data security risks
- apply security measures
- create a positive security culture
- mature their protective data security capability

Organisations not directly in scope for Part 4 of the PDP Act, should still consider the VPDSF and accompanying security Standards as best practice, and align with the security conditions set out in the guidance material where possible. N.B. Public sector organisations not in scope for Part 4 of the PDP Act still retain data security obligations for personal information under IPP 4.

Evidence of Information Privacy and Security

Examples of evidence supporting information privacy and security include the following:

- The organisation is actively implementing requirements outlined in the *Victorian Protective Data Security Standards*, the IPPs and the *Victorian Government Cyber Incident Management Plan*.
- The organisation has information privacy and security strategies in place.
- The organisation has conducted privacy impact assessments and security risk assessments.
- The organisation has appropriate plans in place which are reviewed and maintained (such as a *Protective Data Security Plan* and *Cyber Incident Response Plan*).
- The organisation has clear procedures and points of contact to seek out guidance regarding information privacy and security, and cyber security.
- Protective measures are embedded in day-to-day processes to prevent privacy and security breaches and incidents.
- If incidents occur within the organisation, they are reported in alignment to requirements of the *Information Security Incident Notification Scheme*.

Victorian Government Resources

Resource	Link
<i>Victorian Protective Data Security Framework</i> OVIC	https://ovic.vic.gov.au/data-protection/framework-vpdsf/
<i>Victorian Protective Data Security Standards</i> , OVIC	https://ovic.vic.gov.au/data-protection/standards/
Data Protection, OVIC	https://ovic.vic.gov.au/
Privacy, OVIC	https://ovic.vic.gov.au/
<i>Information Privacy Principles</i> , OVIC	https://ovic.vic.gov.au/privacy/for-agencies/information-privacy-principles/
<i>Victorian Government Cyber Incident Management Plan</i> , DPC	https://www.vic.gov.au/cyber-incident-management-plan
<i>Information Security Incident Notification Scheme</i> , OVIC	https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/incident-notification/
<i>Privacy and Data Protection Act 2014</i>	www.legislation.vic.gov.au