



**Office of the Victorian  
Information Commissioner**

# **PRACTITIONER GUIDE:** **Identifying and Managing Information Assets**

- **Conducting an information review**
- **Defining information assets**
- **Establishing an Information Asset Register (IAR)**

*(Formerly Chapter 1 of the Information Security Management Collection)*

Version 2.0 November 2019

Published by the Office of the Victorian Information Commissioner

PO Box 24274

Melbourne Victoria 3001

First published June 2016

Amended November 2019

Also published on: <https://ovic.vic.gov.au>

ISBN 978-0-6486723-3-3



You are free to re-use this work under a Creative Commons Attribution 4.0 licence, provided you credit the State of Victoria (Office of the Victorian Information Commissioner) as author, indicate if changes were made and comply with the other licence terms. The licence does not apply to any branding, including Government logos.

**Practitioner Guide Details**

<b>Identifying and Managing Information Assets</b> <i>(formerly Chapter 1 of the VPDSF Information Security Management Collection)</i>	
Protective Marking	N/A
Approved for unlimited public release	<i>Yes – Authorised for release</i>
Release Date	November 2019
Review Date	November 2020
Document Version	2.0
Authority	Office of the Victorian Information Commissioner (OVIC)
Author	Information Security Unit – OVIC

For further information, please contact the Information Security Unit on [security@ovic.gov.au](mailto:security@ovic.gov.au)

## Table of Contents

<i>VPDSF Practitioner Guide Details</i> .....	3
1. <i>Background</i> .....	6
2. <i>Purpose</i> .....	6
3. <i>Audience</i> .....	6
4. <i>Use of specific terms in this document</i> .....	6
4.1. <i>What is an information asset</i> .....	6
5. <i>Scope</i> .....	7
6. <i>With thanks</i> .....	8
7. <i>Legislative and regulatory obligations</i> .....	8
7.1. <i>Understand legislative and regulatory context</i> .....	8
7.2. <i>Legal and regulatory references</i> .....	8
8. <i>Information Review</i> .....	10
8.1. <i>What is an information review?</i> .....	10
9. <i>Conducting an information review</i> .....	11
<i>Action 1 – Define the scope of the information review</i> .....	12
<i>Initial review scope (Phase 1)</i> .....	12
<i>Subsequent (broader) review scope (Phase 2)</i> .....	12
<i>Action 2 – Establish a sponsor for the information review</i> .....	12
<i>Action 3 – Identify key personnel (roles and responsibilities)</i> .....	13
<i>Action 4 – Draft communications</i> .....	13
<i>Action 5 – Determine how responses from the business will be collected and recorded</i> .....	13
<i>Action 6 – Review existing resources</i> .....	14
<i>Action 7 – Engage stakeholders and provide ongoing support</i> .....	15
<i>Action 8 – Review responses and record outcomes into the IAR</i> .....	16
10. <i>Define the organisation’s information assets</i> .....	16
10.1. <i>How to define an information asset</i> .....	16
10.2. <i>Logically grouping material into a broader information asset</i> .....	16
10.3. <i>What to consider when defining information assets</i> .....	17
11. <i>Information Asset Register (IAR)</i> .....	17
11.1. <i>What is an Information Asset Register?</i> .....	17
11.2. <i>Business benefits of an IAR</i> .....	17
11.3. <i>Developing an organisational IAR</i> .....	18

<i>11.4. What to include in an organisation’s IAR</i> .....	18
<i>11.5. Selecting an IAR tool</i> .....	18
<i>11.6. OVIC’s sample IAR template</i> .....	19
<i>12. Continually review, validate and update the IAR</i> .....	19
<i>12.1. Key changes</i> .....	20
<i>12.2. Review governance arrangements</i> .....	20
<i>12.3. Manage changes</i> .....	21
<i>12.4. Consider information management requirements</i> .....	21
<i>Appendix A – Sample questions for an Information review</i> .....	22
<i>Appendix B - Example Information Assets</i> .....	23
<i>Appendix C – Sample VPDSF IAR template</i> .....	24
<i>Appendix D – Information Asset considerations</i> .....	25
<i>Appendix E – Suggested Information Management roles and responsibilities</i> .....	28
<i>Information owner</i> .....	28
<i>Information steward</i> .....	28
<i>Information custodian</i> .....	28
<i>Information users / administrators</i> .....	28

## 1. Background

The Office of the Victorian Information Commissioner (OVIC) issues security guides to support the Victorian Protective Data Security Standards (VPDSS). All guidance documents and references are inter-linked and should not be read in isolation.

This document forms part of a suite of supporting security guides of the VPDSS.

## 2. Purpose

This document provides a structured approach for Victorian public sector organisations to:

- identify what information assets they have (conduct an information review)
- articulate and define their information assets
- collectively record and manage their information assets (establish an information asset register)

## 3. Audience

This document is intended for Victorian public sector organisations (including employees, contractors and external parties) that are subject to the protective data security provisions under Part Four of Victoria's Privacy and Data Protection Act (2014).

This guide is designed to support practitioners and information security leads.

## 4. Use of specific terms in this document

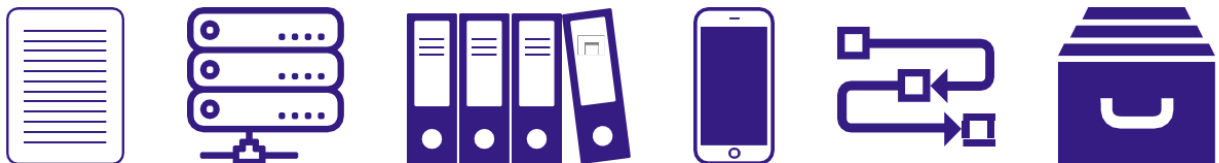
Please refer to the *VPDSF Glossary of Protective Data Security Terms* for an outline of terms and associated definitions. For a current copy of this document, please refer to the VPDSF Resources section of the OVIC website.

### 4.1. What is an information asset

An information asset is described as 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 (i.e. both paper based as well as electronic material).

Information assets have a recognisable and manageable value, risk, content and lifecycle.

An information asset can be a specific report, a collection of reports, a database, information contained in a database, information about a specific function, subject or process.



## 5. Scope

This document directly supports the VPDSS information security standards, and also forms the foundational steps for the VPDSS Five Step Action Plan<sup>1</sup>. Additionally, the activities set out in this document will assist an organisation in:

Developing its Security Risk Profile Assessment (SRPA) and Protective Data Security Plan (PDSP).	OVIC
Meeting the requirements of the IM STD 03 Information Management Governance standard	DPC
Helping inform what information (datasets) might be suitable for release under the DataVic Access Policy and associated Guidelines	DPC
Identifying high value and high-risk information assets that impact the business	PROV & OVIC
Identifying which information assets have the potential to be shared and integrated, inform decision making and offer insight (supporting key outcomes of the Victorian Government IT Strategy)	DPC
Managing public records and implementing disposal programs in accordance with the Public Records Act (1973) and Public Record Office Victoria Standards	PROV
Considering what release provisions relate to specific information assets, set out under the Freedom of Information Act (1982)	OVIC
Adhering to the requirements set out under Part II of the Freedom of Information Act (1982) which requires the publication of information concerning functions, etc. of agencies by comprehensively listing the material it holds.	OVIC

The activities set out across the following document are predicated on organisations having basic records and information management practices in place, and these practices operating effectively.

Public Record Office Victoria (PROV) sets standards for the efficient management of public records under Section 12 of the Public Records Act 1973. The standards apply to all records created by the Victorian Government and detail requirements for the creation, maintenance and use of these records. This guidance supports the PROV standards, based on essential recordkeeping activities.

Organisations should look to PROV material for further guidance on good records management principles and practices. Organisations who have Information or Records Managers will be well placed to help drive the actions set out in this document.

---

<sup>1</sup> Refer to the VPDSS Five Step Action Plan for further guidance on each of the steps. The Five Step Action Plan sets out five recommended steps helping inform the development of an organisations Protective Data Security Plan and secure its information assets.

## 6. With thanks

OVIC would like to acknowledge the assistance given in the development of this guide by the Public Record Office Victoria, DataVic Access Policy Team, Enterprise Solutions Branch (Department of Premier and Cabinet), Victorian Auditor-General’s Office, Victorian Centre for Data Insight, Victorian Information Management Group and the Information Management teams within the Victorian Department of Health and Human Services, Department of Education and Training, and Department of Justice and Community Safety.

## 7. Legislative and regulatory obligations



### 7.1. Understand legislative and regulatory context

Before undertaking any of the suggested activities or actions outlined in this document, an organisation should first consider the legal and regulatory environment in which they operate. This includes understanding any governance arrangements that an organisation has in place, addressing the management and registration of its information assets. These details will help inform the development of an organisation’s own information asset register (IAR) and inform what details are ultimately recorded in the IAR.



A sample IAR template is provided as a supplementary resource, but the fields outlined in this template are not mandatory. Instead, organisations are encouraged to consider their own business requirements to determine the best way to register and manage its information assets.

### 7.2. Legal and regulatory references

The table below provides sample legal, regulatory and administrative requirements governing the management of information assets in Victorian Government. This is not an exhaustive list but acts as a reference point for an organisation to consider. Some organisations may find they have additional requirements that have not been presented in this table, whereas other organisations may identify some of references captured below do not apply to their particular agency or body.

REFERENCE	TITLE / DESCRIPTION
	<p><b>Victorian Protective Data Security Standards (VPDSS)</b></p> <p>The VPDSS establish high level mandatory requirements to protect public sector information across all security areas including governance, information, personnel, Information Communications Technology (ICT) and physical security.</p>
	<p><b>Public Record Office Victoria (PROV)</b></p> <p>PROV standards and policies assist Victorian government bodies with managing their information assets in accordance with the Public Records Act (1973).</p>



	<p><b>DataVic Access Policy (DataVic)</b></p> <p>The DataVic Access Policy is applicable to all agencies (that is, all Departments and Public bodies) of the State<sup>2</sup>.</p>
	<p><b>Freedom of Information (FOI)</b></p> <p>The Freedom of Information Act (1982) applies to Victorian state and local government agencies. This includes Ministers, State Government departments, local councils, public hospitals, most semi government agencies and statutory authorities.</p> <p>Under Part 2 of the FOI Act, organisations are required to identify their information assets for material to be released under FOI.</p> <p>Establishing an organisational IAR will help achieve this.</p>
	<p>Whole of Victorian Government (WoVG) Information Management Governance Guideline (under the Information Management Framework) which requires Departments to implement an IAR that:</p> <ol style="list-style-type: none"> <li>a. registers all significant information assets</li> <li>b. identifies and flags all critical information assets</li> <li>c. is accessible to all staff within your department</li> <li>d. assigns each information asset an owner and custodian (or equivalent)</li> <li>e. complies with the Information Asset Register Standard (under development)</li> <li>f. complies with Part II of the Freedom of Information Act 1982.</li> <li>g. Former WOVG SEC STD 02 – Critical Information Infrastructure (CII)</li> </ol> <p><i>Enterprise Business Solutions (ESB) has confirmed that WoVG Sec STD 02 has been withdrawn with reference to this document and the VPDSF sample Information Asset Register.</i></p> <p><i>Any former requirements for an organisation to account for CII material are addressed in the fields outlined in the VPDSF IAR sample template.</i></p>

<sup>2</sup> N.B. ‘Department’ and ‘Public body’ in the context of the Data Vic Access Policy are defined in the Financial Management Act (1994). Public bodies include State business corporations and statutory authorities.’



Victorian Auditor General's Office (VAGO) – Access to Public Sector Information Report (December, 2015)

This report considered access to public sector information (PSI) and whether whole-of-government leadership and oversight has supported improved performance.

“Access to PSI would foster creative, innovative and often unanticipated entrepreneurial activities when businesses and citizens are allowed to use PSI to create products and services. Open access also enhances engagement between citizens and government on critical policy issues leading to broad economic and social benefits.”

## 8. Information Review

### 8.1. What is an information review?

An information review typically involves surveying all areas of the organisation to help identify:

1. what information assets exist, and
2. evaluate how these assets support the business needs of the organisation.

When conducting an information review, it is critical that information is championed as a business asset in its own right, as opposed to simply considering the technology used to capture or manage the material. It is also essential that all business units and relevant stakeholders (i.e. providers who might be in charge of managing or storing the organisations information) are consulted.

Outcomes of an information review will be used to:

- inform how an organisation defines what is and isn't an information asset, and
- record any identified information assets in the organisation's Information Asset Register (IAR)<sup>3</sup>.

Having completed an information review, an organisation is positioned to effectively consider its information security risks. The knowledge gained from this review is an essential input into an organisation's broader risk register, as risk assessments cannot be properly undertaken without first identifying what assets may be at risk<sup>4</sup>.

---

<sup>3</sup> See Section 11 of this document for more information on Information Asset Registers (IARs)

<sup>4</sup> Organisations should refer to the [Victorian Government Risk Management Framework](#) for further information on the risk management process

## 9. Conducting an information review

Information reviews do not have to be conducted in any particular way. How an organisation approaches this activity will depend on its size, complexity, resources and information holdings. It is essential that the review addresses all types of information, irrespective of media or format (i.e. ensuring that all forms of soft and hard copy information are identified).

The following actions provide practical suggestions on how an information review may be completed. Organisation's may wish to add or remove particular activities when conducting their own review, depending on their business requirements.

ACTION NO.	ASSOCIATED ACTIVITY
<a href="#"><u>Action 1</u></a>	Define the scope of the information review
<a href="#"><u>Action 2</u></a>	Establish a sponsor for the information review
<a href="#"><u>Action 3</u></a>	Identify key personnel (roles and responsibilities)
<a href="#"><u>Action 4</u></a>	Draft communications
<a href="#"><u>Action 5</u></a>	Determine how responses from the business will be collected and recorded
<a href="#"><u>Action 6</u></a>	Review existing resources
<a href="#"><u>Action 7</u></a>	Engage all stakeholders and provide ongoing support
<a href="#"><u>Action 8</u></a>	Review responses and record outcomes into the IAR

To assist organisations in completing these actions, a fuller description of each step is set out on the following pages.

## Action 1 – Define the scope of the information review

Check the box once the action is finalised

It may be useful to take a staged approach to the information review project, by splitting up the review into two phases.

### Initial review scope (Phase 1)

Initially focus on core business functions, critical services, high-profile work units or identified areas of risk, prioritising early efforts on the most important business activities and their related information assets.

### Subsequent (broader) review scope (Phase 2)

As resourcing permits, expand the scope of the review to include the broader services and functions of the organisation, and critically consider any supporting information assets.

Organisations should take into account all information sources and locations. This includes:

- hard copy material used / stored at onsite or offsite locations;
- soft copy materials used / stored in locally hosted corporate systems;
- soft copy materials used / stored under offsite cloud hosting arrangements;
- employees who maintain personal custody of the organisation's information (i.e. stored or managed via personally owned ICT media such as USBs, external hard drives, smart devices, etc); and/or
- archived material that may be stored / managed by outsourced service providers.

## Action 2 – Establish a sponsor for the information review

Check the box once the action is finalised

Senior management should confirm any governance or management arrangements prior to the information review commencing. Their direction will form an important basis for the stakeholder engagement activities needed to support the information review and get their buy-in into the project.

To help support the project, a senior manager should sponsor or champion the information review. The sponsor needs to be someone who understands the benefits that the project will deliver and can help support and oversee the project's efforts. An appropriate sponsor may be the Chief Information Officer (CIO), Director, or for smaller organisations the public sector body head.

A briefing paper may help frame expectations, outlining what will be addressed as part of the review. It can also be used as a basis to develop a business case, ensuring appropriate resourcing and funding is allocated to the project or subsequent activities.

**Action 3 – Identify key personnel (roles and responsibilities)**  Check the box once the action is finalised

Now that the project has a sponsor, the project lead needs to find people who can help support them with the review or they need to engage on a detailed level. OVIC suggests that the project lead gains a thorough understanding of any existing information management (IM) or records management (RM) arrangements of the organisation. These arrangements should describe the different IM / RM roles and responsibilities across the organisations, as well as any external stakeholders who support these functions. Each role will play a different part in the assessment, review and management of information across its lifecycle and will be able to provide unique insights into the review. See *Appendix E* of this document for more information on suggested Information Management roles and responsibilities.

**Action 4 – Draft communications**  Check the box once the action is finalised

Draft communications to support the information review. The communications should, at a minimum, ask business units if there are any known or documented information assets within their business area, and provide instructions on how business units can:

- review their information holdings (discovery exercise);
- identify different information attributes; and
- group the material accordingly (i.e. identify collections and group material into an information asset).

**Action 5 – Determine how responses from the business will be collected and recorded**  Check the box once the action is finalised

Prior to conducting an information review, organisations need to determine how they are going to collect responses from different areas of the business. There are a variety of ways this can be done. Each option has benefits and drawbacks. It is up to the business to ultimately choose whatever is easiest to manage.

Options	Considerations
Conduct a survey or send out a questionnaire	Responding to questions can take time and resources, so be mindful of this when drafting requirements. Any subsequent analysis of the responses can also be challenging if the questions are not framed with a clear understanding and purpose in mind.
Conduct interviews or focus groups with stakeholders	Ensuring there is appropriate representation from all areas of the business (including any relevant external stakeholders). Interviews and workshops can take time initially but can be quite effective in addressing multiple queries and providing coaching all at once.

Provide access to, or a copy of, the IAR for users to directly input into it

This will reduce effort in translating a wide variety of responses into a single format but may require additional assistance to helping users understand what each field in the IAR means for their particular information holdings.

See *Appendix A and B* of this document for a set of sample questions and example information assets.

## Action 6 – Review existing resources

Check the box once the action is finalised

Reduce, reuse, recycle existing resources wherever possible.

Some organisations rely on manual processes or tools to help map different information types across different business areas. Other organisations have techniques or tools in place to help monitor their information holdings.

Try to identify any existing resources that may be available across the organisation to assist in identifying what information assets exist. These existing resources may also highlight additional information that the organisation wasn't otherwise aware of and provide a holistic understanding of their information assets.

Existing resources may include:

- existing documentation from previous information audits (maybe recorded in a register or audit report);
- records management system(s);
- information sharing agreements (i.e. Memorandum's of Understanding (MOUs), Letters of Understanding (LOUs), contracts);
- approved retention and disposal authorities (RDAs);
- technical environment registers;
- configuration management databases or asset lists;
- lists of information required to be reported externally (which may be found in contracts / funding documents);
- system registers; and
- older information lists / registers.

N.B. Older information sources may also be used as a 'baseline' for organisations to tailor questions or considerations. Organisations may use this information review to validate the currency of this content or fill in any identified gaps.

**Action 7 – Engage stakeholders and provide ongoing support** Check the box once the action is finalised

It is essential that all areas of the business are consulted in order to gain a proper understanding of the different functions, activities, systems and technologies used across the organisation. Refer to networks of key personnel (owners, stewards, custodians, users, administrators) to push out the information review to the respective work group and business units.

Organisations should consider including external stakeholders (those that either rely on or provide information to different areas of the business) in any discussions. This type of engagement will help inform additional attributes that the organisation may want to record in its information asset register (i.e. informing access requirements).

When conducting the information review, be sure to communicate the business benefits in completing this exercise. These benefits may include:

- providing better visibility on what information assets exist and how these need to be managed (including understanding what tools and measures are required to manage the information and enhance business operations);
- identifying strengths and weaknesses of particular information assets;
- mitigating risks and forming treatment plans (including the prioritisation of any efforts or resourcing to manage these assets);
- managing regulatory requirements for information assets (i.e. records management, FOI, security, open access, etc.);
- archiving or destroying redundant data (material that has no ongoing business benefit and is disposed in accordance with PROV Standards and Policies);
- using existing information assets to their full potential (reducing duplication of effort);
- potential cost savings (information that is rarely or no longer used on a daily basis may be moved to cheaper long-term storage);
- increasing efficiencies (discoverability), effectiveness (information sharing potential), and economic gains (managing risks to the information and using the material to its full potential); and
- assisting with interagency information sharing and interoperability as well as providing a valuable basis for sharing with industry and research partners.

By completing an information review, organisations are properly positioned to understand the potential impact of change on its information assets and make informed decisions about where to prioritise investment in ensuring the continued usability of its information.

If there is resistance from the business in completing the review, use the executive sponsor (identified in *Action 2* of this guide) to support the engagement strategy. Be prepared for questions and requests for additional support and guidance from the business when conducting the information review.

## Action 8 – Review responses and record outcomes into the IAR

 Check the box once the action is finalised

Once the information review has been conducted, responses from the business need to be recorded in the organisation's master Information Asset Register (IAR). *Section 11* of this guide provides additional insight into IARs.

OVIC has provided a sample IAR template (supplied in *Appendix C* of this document) that sets out some of the more common legal and regulatory obligations for the majority of Victorian public sector organisations.

**Important!** If an organisation intends to use the sample IAR template as a basis for their own IAR, the fields need to be tailored to reflect the unique operating requirements of the business, as not all fields on the template will be appropriate, and in some cases others may need to be added.

## 10. Define the organisation's information assets

### 10.1. How to define an information asset

There is no set process on how an organisation defines what is and isn't an information asset, as the definition should reflect the organisation's unique business requirements.

Practically speaking, organisations should define its information assets at a level of granularity that allows any individual components to be managed usefully as a single unit. Too broad and the organisation will not have enough detail to properly manage the material, too fine and it will have thousands of information assets.

The core attributes (or metadata) used to define or describe an information asset will vary from organisation to organisation. These attributes should describe specific features or characteristics of individual information items that can be grouped into a broader form that makes sense to the organisation. This may be based on specific collections, functions, subjects or processes. This broader form is then considered an information asset for that particular organisation.

### 10.2. Logically grouping material into a broader information asset

It is important to establish a baseline of what 'attributes' an organisation expects form the basis of an information asset. By describing this upfront, stakeholders will be able to assess their information holdings in a similar way, and identify and group information that has 'like' or 'related' attributes. Carefully consider drafting these descriptions/definitions, as they will form the basis of any instructions to users in what to included or exclude in their local information review.

1. Start by broadly describing/defining the **core attributes** of what the organisation would expect an information asset to entail.
2. Then **split** the information groupings until they are of a **suitable size** for the organisation to logically manage.

N.B. At times, a piece of information could logically belong in two different information assets, however, try to simply reference these 'linked' information pieces and **nominate a single information asset as the 'master' or 'overarching' information asset**. This will help reduce conflicts around ownership and control, which can lead to potentially complex business relationships.



This initial process can be somewhat complex, as information assets may be made up of individual items that need different solutions to address the same business need.

### 10.3. What to consider when defining information assets

When deciding how to logically group information into a broader information asset it is worth considering:

- the business context in which the material is being used;
- the security value (Business Impact Level assessment outcome) of the material;
- the business classification (records management) of the material;
- any legal, regulatory or administrative obligations surrounding the management or use of the material; and
- any business engagement activities that it may support.

Each of these considerations and supporting comments are captured in *Appendix D* of this document.

**Remember!** There is no right or wrong way to group information assets, however organisations should ensure any information groupings are consistent and relevant to the organisation's operating requirements.

## 11. Information Asset Register (IAR)

### 11.1. What is an Information Asset Register?

An Information Asset Register (IAR) is a tool that organisations can use to record collections of information (information assets) regardless of media or format.

An IAR can help avoid any unnecessary duplication, as it helps identify what information resources exist across the organisation and provides stakeholders with an overview of the information assets under their care.

### 11.2. Business benefits of an IAR

An IAR can be a useful tool for users, managers and the broader business as it supports:

- the foundation and formulation of information management priorities and strategies;
- governance arrangements (identifying at a high-level what information assets exist, the purpose of these assets, and the roles and responsibilities surrounding the access, use and management of the information);
- the identification and management of associated information risks
- quality, evidence-based decisions to deliver efficient, effective and economic business programs;
- the identification of key information assets and systems (basis for business continuity programs and disaster recovery plans);
- preservation and archiving plans for both digital and hard copy material (PROV requirements);
- important conversations regarding the protection of the information (i.e. what security measures are needed to maintain the confidentiality, integrity and availability of the information asset);
- the identification of particular information assets that may be appropriate for public release (in support of the Data Vic Access policy and Freedom of Information (FOI) requirements); and
- communicates back to the business, what information exists across the organisation.

### 11.3. Developing an organisational IAR

Once an organisation has conducted an information review, outcomes need to be recorded in a central register.

To do this, an organisation should design and develop its own IAR where attributed describing each information asset can be captured. The way that an organisation develops its IAR will depend on its business objectives, the resources it has available and the legislative or regulatory requirements that it operates under.

An organisation's IAR needs to be structured in a way that it is easy to see what is affected if there are changes to the information or business.

### 11.4. What to include in an organisation's IAR

In Victorian government, public sector organisations operate under a variety of legal and regulatory obligations that direct how they are expected to access, use, secure and preserve public sector information. These obligations, combined with an organisations specific business needs, form an essential basis for determining what material should be captured, recorded and managed in the organisational IAR.

The following categories offer high-level guidance on what categories an organisations may record in its IAR:

- Overview / Description of the information asset;
- Governance arrangements (roles and responsibilities);
- information security value (Business Impact Level assessment outcomes)<sup>5</sup>;
- Usage, access and release arrangements;
- Coverage;
- Business services; and
- Risks.

Each of these high-level categories are set out in detail in the sample IAR template (refer to *Appendix C* of this document), with particular fields identifying unique details or attributes to list against each information asset. Organisations should also consider any externally sourced or generated material, as it may also need to be recorded within their organisational IAR.

If a business unit is unsure whether something meets the definition of an information asset, record it within the information asset register until such time that it can be reviewed or refined in subsequent assessments.

### 11.5. Selecting an IAR tool

Before building or procuring a tool for an IAR, first consult with the business to see if a tool is already available (i.e. where records of the information assets can be inputted into or extracted from).

Where a tool does not already exist, organisations may look to use a spreadsheet or document as an initial mechanism to record their information holding details. The sample IAR template provided by OVIC is presented in excel format.

---

<sup>5</sup> For more information on how to determine the security value of an information asset refer to the VPDSF Practitioner Guide: Assessing the Security Value of Public Sector Information. For a current copy of this document, please refer to the VPDSF Resources section of the OVIC website.

### 11.6. OVIC's sample IAR template

To assist organisations in developing their own IAR, a sample template has been included in *Appendix C* of this guide. Organisations may use this as a reference when developing their own organisational specific IAR. The sample IAR template, incorporates requirements and recommendations from:

- Victorian Protective Data Security Standards (VPDSS);
- Public Record Office Victoria (PROV);
- DataVic Access Policy;
- Freedom of Information (FOI);
- Privacy;
- Department of Premier and Cabinet – Enterprise Solutions Branch;
- Victorian Centre for Data Insight; and
- recommendations made by the Victorian Auditor General’s Office (VAGO).

Organisations must consider their own specific operating requirements when choosing what requirements to include in their own IAR, adding or removing certain fields as necessary. The sample IAR template does not include all possible fields that may need to be included, as different organisations have different legal and regulatory obligations.

**INSTRUCTIONS - How to use this sample template**

**Prior to using this template, please read Practitioner Guide: Identifying and Managing Information Assets**

All of your organisation has a lot of systems already in place to register your information assets, you are encouraged to use that in the first instance.

If you do have another tool or system already in place to register your information assets, you are encouraged to use that in the first instance.

This template provides 3 options but not across the different tabs for organisations to use. These tabs present different fields to register various attributes of your information assets.

Organisations need to choose which tab is appropriate for their work program, and refer to the fields on that tab.

**How do organisations group together or split out information assets and capture them in an IAR -**

There is no set process to follow when labelling what is and isn't an information asset. Each organisation will have unique information holdings, business requirements and expectations around the management of that material. These differences mean the same businesses will group their information in different ways to others.

Practically speaking, organisations should identify their information assets at a level of granularity that allows any individual components to be managed easily as a single unit. This level of the organisation will not have enough detail to properly manage the material, but the unit will have thousands of information assets.

Organisations may have a regular group of information assets that are used in a consistent way. The business unit may be used to identify the material in a group, and the business unit may be used to identify the material in a group.

The business unit may be used to identify the material in a group, and the business unit may be used to identify the material in a group.

For more guidance on information Asset Registers refer to [Practitioner Guide: Identifying and Managing Information Assets](#)

For more guidance on terms used in this IAR, refer to the [VPSA Glossary](#)

For a current copy of these documents, please refer to the [VPDSS Resources](#) section of the OVIC website.

**Which tabs should you use?**

**VPSA Requirements**

If you are holding an IAR to comply with the VPSA, please use the tab that is:

**COSE (in VPSA only)**

The tab includes a list of fields that organisations should record attributes of their information assets in.

The fields on this tab will help you meet the requirements of the VPSA, as well as other existing legal and regulatory information management (IM) obligations across Victorian Government.

Organisations must consider their specific operating requirements and relevant legislative and regulatory obligations when developing their own specific IAR.

The use fields represent the most common requirements for the majority of Victorian Government agencies or entities.

**AUSTRALIAN PRIVACY**

If your organisation already has an information asset register in place for complying with the *Privacy Act* or another privacy regulation, you are encouraged to use that register.

This tab includes a list of supplementary fields that organisations can consider including in their IAR.

These fields are based on existing legal or regulatory obligations across Victorian Government.

Organisations must consider their specific operating requirements and relevant legislative and regulatory obligations when developing their own specific IAR, as well as their own business needs.

**REQUIREMENTS**

ASSET REGISTER	ASSET IDENTIFICATION	PERSONAL INFORMATION	INTERNAL INTERESTS OR NATIONAL SECURITY INFORMATION (INIS)	LOCATION	FORMAT	CLASSIFICATION (e.g. PROTECTED DATA)	LAST UPDATE	OPERATION	OWNER	CUSTOMER	BUSINESS IMPACT (e.g. REPUTATIONAL RISK)
<b>VPSA</b>	The name of the information asset	Details of the asset and its classification	Is the asset a personal information asset?	Where is the asset held?	What is the format of the asset?	What is the classification of the asset?	When was the asset last updated?	What are the operations performed on the asset?	Who is the owner of the asset?	Who is the customer of the asset?	The business impact of the asset (e.g. reputational risk)
<b>AUSTRALIAN PRIVACY</b>	Asset name	Asset description	Is the asset a personal information asset?	Where is the asset held?	What is the format of the asset?	What is the classification of the asset?	When was the asset last updated?	What are the operations performed on the asset?	Who is the owner of the asset?	Who is the customer of the asset?	The business impact of the asset (e.g. reputational risk)

For more information on the sample IAR template can be found in *Appendix C* of this guide.

### 12. Continually review, validate and update the IAR

An organisation should regularly review the status of its information assets and update both the content within the IAR as well as the IAR fields themselves, at least annually, or if there is a significant change to the organisation’s risks or operations. This will ensure the currency of the IAR content, as well as being able to amend or update information asset management plans to reflect any changes or developments in the organisation’s core business.

### 12.1. Key changes

When reviewing the IAR, consider changes to:

- the status (i.e. current, semi current or non-current material or perhaps legacy information);
- the legal or regulatory environment in which the organisation operates;
- any information inputs or outputs (e.g. new or updated information sharing arrangements, cessation of existing arrangements; the provision or receipt of information based on new or updated engagements with external parties or contracted service providers);
- the frequency of publications and the currency of the content in the IAR;
- the security value of the information<sup>6</sup>;
- confidentiality requirements of the material - if the confidentiality conditions are reduced, then this may introduce information release opportunities;
- interoperability opportunities - organisations should consider the overlaps between information processes, program management and project management methodologies, as well as any business process improvement initiatives to ensure that the currency of their information assets is maintained. For example, a project may need to update the organisation's IAR and their associated roles and responsibilities due to the implementation of business processes and systems that create or use new information assets;
- contracted service provider (CSP) arrangements and any inputs they may have to the IAR content or requirements. CSP arrangements can include external personnel working with the organisation's information or looking after the organisation's infrastructure or systems (e.g. outsourced ICT providers); and
- definitions and groupings as these may also change over time (e.g. a particular project's information assets may contain archived items that have been moved in long-term storage. Throughout the project lifecycle more material is created and other material is no longer actively used. This inactive material may be added to the archived information asset, which may continue to grow over time). Alternatively, the organisation may refine the way in which it articulates or defines an information asset, introducing additional granularity in its description. These changes need to be reflected in the IAR as definitions and groupings naturally evolve.

### 12.2. Review governance arrangements

Organisations should ensure that the IAR is itself recorded as an asset in the IAR<sup>7</sup>, as well as defining a permanent owner and respective custodian of the IAR. This could be the organisation's CIO or information manager (as opposed to owners of the particular information assets described within it) who is ultimately accountable for the oversight, management and maintenance schedule for the register as well as ongoing engagement with the business.

Depending on arrangements within the organisation, the project lead may also consider identifying responsible officers in each business unit to maintain the currency of each unit's input to the IAR. This will assist in ensuring that the information assets identified in the register are appropriately recorded, stored and maintained, and are accurate and not unnecessarily duplicated.

---

<sup>6</sup> Refer to VPDSF Practitioner Guide: Assessing the Security Value of Public Sector Information, for instructions on how to assess the security value of information. For a current copy of this document, please refer to the VPDSF Resources section of the OVIC website.

<sup>7</sup> The IAR is a permanent record under PROS 07/01 General Retention and Disposal Authority for Records of Common Administrative Functions Version 2009 RD.

Should roles and responsibilities across the organisation change, these details also need to be updated in the IAR. This may be due to new delegations being introduced, additional or discontinuation of particular roles or functions.

If the organisation undergoes a significant change to its operating environment (like a machinery of government change prompting a merger or disassembly of some areas of the business) then these details also need to be updated and reflected in the IAR.

### **12.3. Manage changes**

Once an organisation has developed a comprehensive understanding of its current information assets and any associated requirements, it will find itself much better placed to assess how these changes could affect its information assets. Changes may include adjustments to the information assets themselves, how they are managed, adjustments to the technology supporting them or the business requirements driving them.

For specific changes, organisations should undertake impact and risk assessments to identify appropriate mitigation actions and treatment plans. An organisation may also use this information to improve its change management processes and assist with future change planning.

Finally, the organisation must ensure that the management of the IAR itself is considered within broader organisational change management processes. If the IAR is not updated when changes occur, it becomes redundant, misleading and not used to its full potential.

### **12.4. Consider information management requirements**

Alongside having the right tools to support the organisation's information requirements, there are likely to be information management processes needed to support the delivery of the requirements.

The creation of an organisational IAR and the process of assigning appropriate governance roles may highlight to responsible personnel their obligations and outcomes in managing and maintaining these information assets. This may mean crafting guidance on how to meet these obligations, such as updating and/or enforcing metadata, information access and release policies, security policies, or providing relevant training and guidance on how and where to store information.

### Appendix A – Sample questions for an Information review

The below table presents sample questions that may be used in a broader questionnaire as part of an information review.

SAMPLE QUESTIONS	COMMENTS
What are the core information assets created or used in each business area?	Request a title and description (overview) of each information asset
What format is information stored in (soft or hard copy)?	For soft copy material, identify what digital format this takes (e.g. doc, ppt, xls)
Where is the information stored? i.e. a shared drive, database, EDRMS, or physical location if in hard copy form?	Request details of the soft copy location (i.e. pathway) or physical storage location of where the material is actively used
Who are nominated owners and custodians of the information asset?	Request a title and contact details for each information asset
What is the status of the information asset?	i.e. is the information current, semi current or non-current material and considered legacy information?)
What is the assessed business impact level (BILs) for the information asset?	This involves an assessment of potential compromise to public sector information – confidentiality, integrity and availability and applying a BIL rating <sup>8</sup>
Is the information used as input or output of a business process?	Request a brief description of the business processes
Is the information used in a decision-making process?	If yes, request a brief description of the business making processes
Is the information used to evaluate a business rule or condition?	If yes, request a brief description of the business rule
Is the information subject to any information sharing agreements or arrangements (this can be formal or informal)	If yes, request a brief description of the agreements or arrangements

<sup>8</sup> See VPDSF Practitioner Guide: Assessing the Security Value of Public Sector Information for instructions on how to assess the security value of information using the VPDS Business Impact Levels (BILs).

## Appendix B - Example Information Assets

The following high-level information assets are offered purely as examples. Depending on how an organisation defines its information assets, as well as its understanding of its information holdings will inform what material is ultimately recorded in the organisational IAR.

SAMPLE INFORMATION ASSETS	COMMENTS
A database of contacts	Each entry in the database may not need to be treated individually; the collection of data may therefore be considered one information asset. All the individual records within the asset will have similar risks associated with privacy and storage of personal information.
All files associated with a specific project	This might include spreadsheets, documents, images, emails to and from project staff and any other form of records. All the individual items may be gathered together and treated the same as they have similar definable content, and the same value, business risk and lifecycle.
Financial information	This could include invoices, receipts, accounts, delegations, or financial statements, or it may simply refer to all the financial information for the organisation. There are very specific risks to the business if this information is mismanaged and organisations may also have an obligation to provide transparency of information, which could be problematic.
HR records	These can be collections of hard and soft copy communications and documents related to the employment of an employee stored under the person's name or identification number, including but not limited to forms, letters, memos, reports, lists, e-mails, etc. The records serve as the historical record of information pertaining to an employee from date of hire to separation and contain some pre-employment and post-employment information. This can also include records covering employment, position classification, wage or salary, employee relations, performance management, training, organisational development, attendance and paid time-off usage, etc.
Budget papers	This may consist of the budget speech, budget highlights, four budget papers, Ministerial statements, and portfolio budget statements. Ministerial media releases and budget kits can also be useful sources of information.

### Information that should not be considered an information asset

Systems, applications and databases that collect, manage or store information are not information assets, however the information contained within them is. The level of granularity that an organisation defines its assets may evolve, as the organisation matures in its understanding of what it has.

It is unlikely that an organisation could treat all the content in its records management system as a single asset as the content is likely to cover a diverse range of unrelated topics, each requiring different maintenance and management. Depending on the content in the system, certain records may be grouped into similar types and ultimately considered an information asset.

It is important to note that ‘Unofficial’ information (such as personal correspondence) should not be considered an information asset of the business, despite sometimes being captured on official organisational systems (i.e. email systems).

**Appendix C – Sample VPDSF IAR template**

A copy of the most current downloadable excel spreadsheet forming the IAR template is available under the VPDSF Resources section of the OVIC website.

The screenshot displays the OVIC Sample Information Asset Register (IAR) Template. It features an 'INSTRUCTIONS' tab and a 'REQUIREMENTS' tab. The 'REQUIREMENTS' tab is active, showing a table with columns for ASSET NAME, ASSET DESCRIPTION, PERSONAL INTEREST, NATIONAL INTEREST, LOCATION, POWER, CREATION DATE, LAST UPDATED, ORIGINATOR, OWNER, CUSTOMER, and BUSINESS IMPACTED BY. The table includes detailed instructions for each field, such as 'The name of the information asset' for ASSET NAME and 'The date when the information asset was created' for CREATION DATE. The instructions also reference various legislative and regulatory requirements, including the Victorian Privacy Act 2014 and the Victorian Information Privacy Act 2014.

**Note** – Ensure you read the ‘How to use this sample template’ tab, before filling in the sample IAR template. This tab describes what is captured in the sample spreadsheet. All three tabs do not need to be completed!



- The **VPDS requirements** tab includes the minimum fields that an organisation should register for each information asset, for the VPDS
- The **Core and Supplementary** tabs outline additional IM references and considerations that organisations may look to include in their own organisational specific IAR.

To download a copy of the sample excel IAR spreadsheet please refer to the VPDSF Resources section of the OVIC website.



Appendix D – Information Asset considerations

INFORMATION ASSET CONSIDERATIONS	SUPPORTING COMMENTS
<p>Business engagement</p>	<p>Consider how each of the business units currently use or engage with certain pieces of information in their day-to-day work. This engagement may assist in logically grouping individual items into a broader information asset that reflects operational business needs. Some probing topics and associated questions to consider include -</p> <ul style="list-style-type: none"> <li>• the use of ‘like’ or ‘related’ material doesn’t have to be based on an ICT system or application, but may be informed by a business, function or activity</li> <li>• usability covers everything from discoverability of the information, through how the information assets are accessed and what is done with them</li> <li>• current information usage requirements, as well as future requirements (these may change over time)</li> <li>• operational record requirements (i.e. retention and disposal authorities issued by the Public Record Office Victoria) may also influence an assessment or grouping of the information asset, as well as informing retention timeframes and application of security measures across the information lifecycle</li> <li>• the functionality that the organisation requires from its information, how the material is used and what the organisation needs to do with it, e.g. create, modify, access, sort, store, transmit -             <p style="margin-left: 40px;">For example, it is unlikely that the organisation will treat all the content in its large information storage system such as a records management system or data warehouse as a single information asset. These systems or holdings are likely to cover a diverse range of unrelated topics, which can mean different measures (including security measures) are needed to properly manage this information across its lifecycle. Depending on the content, certain records may be grouped into similar types.</p> </li> </ul> <ul style="list-style-type: none"> <li>• How does the business use or work with the information?</li> <li>• What does the business need to do (functionality, business services, etc.) with the information?</li> <li>• What tools (this can be systems, hardware or software) are needed to work with the information?</li> <li>• How can the information be accessed?</li> <li>• What technologies, configurations and management processes</li> </ul>

	<p>are in place to access the information?</p> <ul style="list-style-type: none"> <li>Who needs to access certain pieces of information (i.e. ‘need to know’ principle, or perhaps personnel security checks are required for access to this information)?</li> </ul> <p>N.B. If everything within the information asset is security classified, only those with the right security clearance are authorised to access or use that information.</p> <p>Alternatively if only some of the records within the broader information asset are security classified then the business needs to consider how to manage access to these records without restricting access to the rest of the information asset.</p> <ul style="list-style-type: none"> <li>How will an organisation enable people to find the information in the way they need it?</li> <li>Granularity and depth of the discoverability (search) required will depend on the type of asset; it may involve finding the asset itself, searching within the asset for files, or searching within those files to find specific pieces of data. This is both about the technology actually used to search for information and also the technology that is used to store the information.</li> </ul>
<p>Business context</p>	<p>Consider the business context and environment in which the organisation operates. This may drive the way in which the information assets are defined and the subsequent implementation of security measures to protect this material.</p> <p>The nature, size and functions of an organisation will also influence the types of information assets it has.</p>
<p>Legal or regulatory obligations</p>	<p>Consider any legal or regulatory obligations that the organisation has, as these existing requirements may inform how the organisation records information elements or structures particular information sets.</p> <p>An example of this may include existing obligations under the DataVic Access Policy<sup>9</sup>. Under this policy, an organisation may already be capturing metadata elements that can help categorise and define additional information assets.</p>
<p>Business classification (records management)</p>	<p>Check if any of the records have a registered business classification, as this can act as a useful basis to understand various information elements (i.e. information linkages, grouping, naming, vital records, user permissions, retrieval, disposition and identification of vital records).</p>

<sup>9</sup> Organisations publishing datasets on the DataVic portal should consider the [‘Dataset Publishing manual’](#)

	<p>If a record has been registered under a business classification<sup>10</sup>, consider the assessment process and any information that accompanies this record. Business classification schemes assist with identifying the scope, types, use and functions of an organisation’s information assets and can direct accessibility and re-usability of the material. Common business classification categories can include:</p> <ul style="list-style-type: none"> <li>• Committees</li> <li>• Employee relations</li> <li>• Government relations</li> <li>• Information management</li> <li>• Legal services</li> <li>• Operations management</li> <li>• Policies and procedures</li> <li>• Procurement</li> <li>• Risk management</li> <li>• Property management</li> <li>• Strategic management</li> <li>• Technology and telecommunications</li> <li>• Work Health and Safety</li> </ul> <p>N.B. Business classifications are different to security classifications</p>
<p>Externally sourced information</p>	<p>Organisations should take into account any externally sourced or generated information, as it may also be considered an information asset of the business depending on:</p> <p>the functions, processes or activities that this material is supporting;</p> <p>what other information this material is combined with; and</p> <p>terms of the agreement or arrangement under which the material is supplied (i.e. does the organisation maintain ownership and IP over the information or is the organisation permitted to use this material under a copyright agreement).</p>

---

<sup>10</sup> Business classifications are designed to support the records management needs of an organisation and act as a means of arranging records in a logical structure and sequence, facilitating their subsequent use and reference (PROS 11/09: Control Standard – 2.2 Classification). On the other hand, security classifications are used to identify information that has heightened confidentiality requirements.

## Appendix E – Suggested Information Management roles and responsibilities

The following list sets out some of the more commonly recognised IM roles and associated responsibilities. Not all organisations will have these particular roles, or even describe these functions in the same way, with some smaller organisations perhaps having a single person performing a few functions. It is expected that organisations define their respective roles and responsibilities based on relevant legislative and / or regulatory obligations.

### Information owner

An information owner is the person or entity that has legal possession of the information asset and are ultimately accountable for that information. For some organisations this may be the agency or body for which the information asset was produced or acquired, and in turn the public sector body head who retains ownership of the organisation's overall information assets. For other organisations, ownership may be defined in particular legislative instruments.

In some organisations, it may be appropriate for the information owner to delegate the management and handling of responsibilities associated with the information asset to an information steward and / or an information custodian.

### Information steward

In some organisations this may be where an information owner has delegated responsibility for the information asset to an information steward. This person or role is responsible for making sure the asset is meeting its requirements, and that risks and opportunities associated with the information are monitored and managed. The steward, in this instance, has operational accountability for the information.

The information steward need not be the creator (originator) of the information, or even the primary user of the asset, but they must have a good understanding of what the business needs from the information asset, and how the information can help fulfill those requirements.

The information steward is often a subject matter expert, or 'owner' of the relevant business process, for a particular information collection or asset.

The role (or delegate role) should be involved in any risk assessments and analysis of the information to help assess its security value. Only once this assessment has been made, can the relevant security measures be considered to protect the information asset.

### Information custodian

An information custodian is generally described as either a designated person, position, officer, business unit or agency with assigned responsibilities for the information asset to ensure that the information is managed appropriately over its lifecycle, in accordance with rules set by the information owner or steward and the quality of information is assured.

### Information users / administrators

Any person who generates or receives public sector information. This can include staff or external parties who have access to the information.