

# Public Record Office Victoria Report

**Information Management Maturity Assessment Program 2023-24**

## **Report Part Three A: Data Management Results Supporting Comments**

## IMMAP Report 2023-24 Part 3A Data Management Comments Version 2: Deidentified

### Document information

Version	<i>V1.0 FINAL</i>
Approved by	<i>Justine Heazlewood, Director, and Keeper of Public Records</i>
Date	06 June 2025
Business owner	<i>Alison McNulty, Acting Assistant Director, Government Services</i>
Authors	<i>Xander Hunter, Manager, Standards and Policy</i>
Classification	<i>OFFICIAL</i>

### Copyright Statement

© State of Victoria through Public Record Office Victoria 2025



Except for any logos, emblems, and trademarks, this work 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 Report.

# Table of Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	Report overview	4
1.2	Scope	4
<b>2</b>	<b>D1: People</b>	<b>5</b>
2.1	People: 1.1 Data literacy and responsibility	5
2.2	People: 1.2 Capability and capacity	9
2.3	People: 1.3 Training, support and knowledge sharing	12
<b>3</b>	<b>D2: Organisation</b>	<b>16</b>
3.1	Organisation: 2.1 Governance	16
3.2	Organisation: 2.2 Vision and strategy	18
3.3	Organisation: 2.3 Strategic alignment	20
3.4	Organisation: 2.4 Management, advocacy and leadership	22
3.5	Organisation: 2.5 Audit and compliance	25
<b>4</b>	<b>D3: Lifecycle and Quality</b>	<b>29</b>
4.1	Lifecycle and quality: 3.1 Asset management	29
4.2	Lifecycle and quality: 3.2 Policies and procedures	32
4.3	Lifecycle and quality: 3.3 Meeting business and user needs	35
4.4	Lifecycle and quality: 3.4 Accessibility, discoverability, and availability	37
4.5	Lifecycle and quality: 3.5 Data use and reuse	40
<b>5</b>	<b>D4: Business Systems and Process</b>	<b>44</b>
5.1	Business systems and processes: 4.1 Data architecture	44
5.2	Business systems and processes: 4.2 Process improvement	46
5.3	Business systems and processes: 4.3 Business systems and tools	48
5.4	Business systems and processes: 4.4 Privacy and security	50
<b>6</b>	<b>D5: Data Integrity (Optional)</b>	<b>55</b>
6.1	Data integrity: 5.1 Sharing, access, integration and interoperability	55
6.2	Data integrity: 5.2 Open data	57
6.3	Data integrity: 5.3 Data and AI ethics	58
6.4	Data integrity: 5.4 Data quality	60
6.5	Data integrity: 5.5 Data availability	62
6.6	Data integrity: 5.6 Indigenous Data Sovereignty	65

# 1 Introduction

## 1.1 Report overview

The 2023-24 IMMAP Report is divided into the following parts:

- Part One: Consolidated Results: includes recommendations
  - Part One A: Executive Summary
  - Part One B: IMMAP Methodology
  - Part One C: Context
- Part Two: Information Management: by Question
  - Part Two A: Supporting Comments
  - Part Two B: Information Management Questionnaire
- Part Three: Data Management: by Question
  - **Part Three A: Supporting Comments (this part)**
  - Part Three B: Data Management Questionnaire

Public Record Office Victoria (PROV) would like to acknowledge the continuing support and engagement of the participating organisations in IMMAP. Without their willingness to bring honest evaluations of their information and data management maturity to the table, the IMMAP reports would not be the valuable resource and planning tools they are.

## 1.2 Scope

This part of the report (**Part Three A: Supporting Comments**) contains a collation of the evidential comments made by participating organisations to support each rating.

Any de-identifying changes made to the comments are placed in square brackets []. For example, references to Department or a specific agency in the comments have been adjusted to [Organisation]. Where a shared service completed IMMAP submissions for multiple organisations, supportive comments provided for those organisations may appear to be duplicated or very similar. The duplicated or similar comments were not weeded out for completeness. Some small corrections to spelling or grammar were undertaken where needed, otherwise comments remain mostly as they were provided in the responses submitted.

Ratings assigned by participating organisations for the 23 data management questions asked across the four dimensions of People, Organisation, Lifecycle and Quality, and Business Systems and Processes, along with the optional fifth dimension of Data Integrity, are provided in **Part Three: Data Management**. The optional fifth dimension does not have a corresponding set of information management questions. Two organisations opted out of dimension five, and are not included in assessment responses for the corresponding six Data Integrity questions.

A copy of the questionnaire containing the Data management questions from the Information Management Maturity Measurement (IM3) Tool<sup>1</sup> used to assess maturity is located in **Part Three B: Data Management Questionnaire**.

---

<sup>1</sup> <https://prov.vic.gov.au/recordkeeping-government/learning-resources-tools/information-management-maturity-measurement-tool-im3>

## 2 D1: People

Responding organisations provided supporting explanatory text for assigned ratings.

### 2.1 People: 1.1 Data literacy and responsibility

#### From the questionnaire

Question:

- Do the staff in your organisation demonstrate awareness of their data management responsibilities and are they commensurate to their roles?
- What is the current level of data literacy held by staff in your organisation?
- Do staff in your organisation value data as an asset?

Examples of evidence:

- A custodianship model has been deployed that identifies the roles and responsibilities of staff in relation to the organisation's data assets.
- Staff demonstrate that they are aware of the importance of data management to the organisation and of their responsibilities in relation to it.
- Staff data management roles and responsibilities are defined in documentation such as policies and job descriptions and are commensurate to their roles.
- Staff are aware of and act in accordance with the Victorian Public Sector Code of Conduct requirements regarding data. Staff manage data in line with organisational requirements and use data effectively in a manner that is commensurate to their roles.
- Staff are educated and encouraged to exploit data to the fullest. They actively engage in new data management initiatives and seek better understanding of the organisation's data assets.
- Staff receive training to improve their data literacy and to manage data in line with their role within the organisation.

#### Supporting comments from participating organisations:

[Business area] have procured a data literacy roadmap, but have not had the resources for a wide implementation or rollout at this stage. Across [the Organisation] there are pockets of good practice.

There is a significant focus on being a data driven organisation and there is some resource engaged however overall organisation data literacy or usage opportunities can be improved.

One responding team is a team of data analysts, each team member has an advanced level of general data literacy.

Custodianship models are deployed in several Groups/Divisions to set out responsibilities of staff in relation to data assets.

Some Groups/Divisions employ dedicated data experts and define data management roles and responsibilities in documentation such as policies and job descriptions. In other cases, data analyst type roles e.g. performance reporting, are not necessarily filled by data professionals.

IM related policies and some training in place:

- Information Asset Governance Policy, and supporting information are available on the IM SharePoint site, and are currently under review. Tailored advice/assistance is provided by the Information Management (IM) team.
- Data Access and Release Policy, Data Quality Policy and supporting information are available on the IM SharePoint site and are currently under review. Tailored advice/assistance is provided by the Information Management (IM) team.
- Privacy Policy, Privacy Impact Assessment Guide, reporting and managing privacy incidents guide, developing a collection notice for personal and [business function] information, and supporting information are available on the intranet. Tailored privacy advice and assistance is provided by [the Organisation's] Privacy Team and Legal Services Branch.
- A new suite of Information Security standards address governance, secure handling of information, risk management, training and awareness, incident management, business continuity planning and disaster recovery, working with third parties, logs and monitoring, systems requirements, network security, change and configuration management, personnel and physical security and cryptography. Additional supporting information and training are available on the intranet and Cyber Security SharePoint. Tailored advice and assistance is provided by the Cyber Security team.
- Acceptable use of technology policy.
- Protective Markings guides including how to handle information sensitively and an eLearning module, are available via the intranet.
- People can seek additional advice/support from the Information Management and PowerBI Viva Engage communities.

The Information Asset Register is maintained in SharePoint to improve discoverability. Custodians/delegates responsible for keeping information current.

The Purview Data Catalogue enables [the Organisation] to create and maintain an inventory of data assets, providing context to understand datasets.

The Information Management (IM) SharePoint includes data information and literacy resources.

Data visualisation eLearning and guides for developers and consumers are available in OurPeople learning.

Data Linkage technical specifications, [resources] and [linked datasets] data dictionary, Provisioned Linked data (which provides users with information on IDR characteristics such as conformed variables), and Protocol for Data Collection, linkage, use and release.

The [secure virtual environment] user guide.

The following eLearning modules are deployed to new starters and all staff as part of mandatory compliance training, with a refresher every two years. This training supports staff in understanding their obligations to manage information securely:

- Code of conduct (references using information, recordkeeping, legislative compliance).

- Security Awareness (six modules: Information security obligations, You are the shield, Data security, Social engineering, email and phishing, Targeted attacks).

New staff are onboarded and have access to the 'giving' [Organisations] onboarding and eLearning modules. Most giving [Organisations] do not currently have data literacy as a component of onboarding and eLearning modules.

IM related policies and some training in place:

- Information Asset Governance Policy, and supporting information are available on the IM SharePoint site, and are currently under review. Tailored advice/assistance is provided by the Information Management (IM) team.
- Data Access and Release Policy, Data Quality Policy and supporting information are available on the IM SharePoint site and are currently under review. Tailored advice/assistance is provided by the Information Management (IM) team.
- Privacy Policy, Privacy Impact Assessment Guide, reporting and managing privacy incidents guide, developing a collection notice for personal and [business function] information, and supporting information are available on the intranet. Tailored privacy advice and assistance is provided by [the Organisation's] Privacy Team and Legal Services Branch.
- A new suite of Information Security standards address governance, secure handling of information, risk management, training and awareness, incident management, business continuity planning and disaster recovery, working with third parties, logs and monitoring, systems requirements, network security, change and configuration management, personnel and physical security and cryptography. Additional supporting information and training are available on the intranet and Cyber Security SharePoint. Tailored advice and assistance is provided by the Cyber Security team.
- Acceptable use of technology policy.
- Protective Markings guides including how to handle information sensitively and an eLearning module, are available via the intranet.
- People can seek additional advice/support from the Information Management and Powerbait Viva Engage communities.

The Information Asset Register is maintained in SharePoint to improve discoverability. Custodians/delegates responsible for keeping information current.

A data analytics strategy has been endorsed.

The Purview Data Catalogue enables [the Organisation] to create and maintain an inventory of data assets, providing context to understand datasets.

The Information Management (IM) SharePoint includes data information and literacy resources.

Data visualisation eLearning and guides for developers and consumers are available in OurPeople learning.

PowerBI guides for developers and consumers.

Data Linkage technical specifications, [resources] and [linked datasets] data dictionary, Provisioned Linked data (which provides users with information on IDR characteristics such as conformed variables), and Protocol for Data Collection, linkage, use and release.

The [secure virtual environment] user guide.

The following eLearning modules are deployed to new starters and all staff as part of mandatory compliance training, with a refresher every two years. This training supports staff in understanding their obligations to manage information securely:

- Code of conduct (references using information, recordkeeping, legislative compliance).
- Privacy awareness.
- Security Awareness, including 6 modules: Information security obligations, You are the shield, Data security, Social engineering, email and phishing, Targeted attacks.

Evidence and Insights are highly literate in understanding their responsibilities with regards to data management. Next Gen are in a formative level of maturity in terms of data literacy and are progressing with addressing roles and responsibilities around data management. The remainder of [the Organisation] is at various levels of aware maturity. This is being addressed primarily through the guardrail processes associated with application upgrade and rollout. None of these have identified specific data management roles and responsibilities.

Staff manage information in line with organisational requirements and use information effectively in a manner that is commensurate to their roles. Innovative approaches to use of information are being considered. Information Asset Register has roles and responsibilities. Training is provided as part of records management system upgrade.

[The Organisation] does not currently have data literacy as a component of onboarding and eLearning modules.

Currently no dedicated data literacy education program or products are in place.

Staff are aware of and act in accordance with the Victorian Public Sector Code of Conduct requirements regarding information.

There are mandatory training sessions on data management, data management policies and procedures, recruitment of data management SMEs Roles for various datasets are identified before cataloguing.

Endorsed Data form where stakeholder are all divisions.

Currently Establishing data working group with regular workshops with subject matter experts across the organisation to understand current challenges. Evidence of good literacy in some areas while other areas require uplift. Identified training needs and requirements enterprise wide with respect to the IM Framework and specific data roles, training program with ongoing monitoring, review and update existing training content to uplift/streamline data handling modules. Approved Data Governance Framework including awareness enterprise wide.

## 2.2 People: 1.2 Capability and capacity

### From the questionnaire

Question:

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

Examples of evidence:

- Strategies and/or programs of work have been implemented to address any gaps in data management skills, capability, and capacity.
- The organisation gives priority to recruiting specialists to help develop the organisation's data management and utilisation capability (e.g., Data Analysts).
- The human resources requirements for data management are regularly assessed in terms of capacity, skills, and knowledge.
- Data management specialists are respected professionals who are consulted in the development and implementation of business initiatives.
- Data management specialists have been appointed into dedicated roles and actively maintain their knowledge and literacy as commensurate to their roles.
- There are enough staff with relevant capability and capacity employed in data management roles in the organisation.
- Data management projects and initiatives are adequately resourced and funded within the organisation.

### Supporting comments from participating organisations:

Ongoing [business area] restructuring activities continue to address [the Organisational] requirements for data management skills, capability and capacity. A number of other areas across [the Organisation] are taking steps to increase their capability to manage and use data effectively.

Whilst there are data management specialists, additional training is required for business unit staff to ensure that data is entered accurately, completely and in a timely manner.

One respondent indicates they are reliant on [the business area] centralised database systems, and there are some limitations to funding of data improvement initiatives.

There is inconsistency across [the Organisation] in how data management is resourced: some Groups/Divisions have employed data specialists into dedicated roles; in other cases, these roles are performed by generalist staff or there are insufficient staff with relevant capability and capacity employed in data management roles.

Information Management and data specialists are recruited to roles that predominately deal with data and information management, including in the [business function] divisions and [business function] branch.

IM team supports staff in other divisions with responsibility for implementing [the Organisation's] IM policies to develop materials and procedures tailored to their business needs.

Data literacy learning and development opportunities are made available through [the Organisation's] training calendar and LinkedIn learning.

Business units who are seeking a technology solution undertake an information security classification exercise to inform the security classification of the information, which in turn guides the solution requirements and the information handling requirements.

Business units that propose projects that involve the collection, use or disclosure of personally identifying information (or changes to existing projects that do these things) may be required to draft a Privacy Impact Assessment to describe the data flows for the project, and they are assisted to identify privacy and information security requirements for the project by legal, information management and cyber security teams.

Programs of work to address DM capability are resourced and funded, within budget constraints, for example implementation of the Enterprise Data Catalogue.

The Information and Data Management Reference Group membership includes information and data management subject matter experts who provide advice and share knowledge.

Staff with records management expertise are available to support procurement of new products requiring record keeping capability and decommissioning of legacy systems where the content requires migration for record keeping purposes.

People can seek additional advice/support from the Information Management and PowerBI Viva Engage communities and the Data Analytics and Insights Community of Practice on the VPS Innovation network.

[The Organisation] has dedicated and specialist data management and analytical staff who liaise with data owners and stewards. These are highly skilled staff.

Information Management and data specialists are recruited to roles that predominately deal with data and information management, including in the [business function] divisions and [business function] branch.

IM team supports staff in other divisions with responsibility for implementing [the Organisation's] IM policies to develop materials and procedures tailored to their business needs.

Data literacy capability is addressed in [the Organisation's] capability framework and learning and development opportunities are available in OurPeople eLearning.

Consultation with data specialists in the development and implementation of business initiatives in the early stages is improving but is not yet established as common practice.

Business units who are seeking a technology solution undertake an information security classification exercise to inform the security classification of the information, which in turn guides the solution requirements and the information handling requirements.

Business units that propose projects that involve the collection, use or disclosure of personally identifying information (or changes to existing projects that do these things) may be required to draft a Privacy Impact Assessment to describe the data flows for the project, and they are assisted to identify privacy and information security requirements for the project by legal, Information and Digital Solutions (IDS) cyber security and (as relevant), Records Management and Procurement.

Programs of work to address DM capability are resourced and funded, within budget constraints, for example implementation of the [central data repository] and Enterprise Data Catalogue.

Greater use of analytical and predictive models to provide business insight, such as the Emergency Demand dashboard (initiated by [the Head of the Public Office]).

The Information and Data Management Reference Group and [business function] Data Governance Group membership includes information and data management subject matter experts who provide advice and share knowledge.

The Analytics Strategy addresses data management capability.

IT System Assessments are delivered by Records Management Unit in collaboration with branch/business unit.

Recordkeeping Assessments delivered by Records Management Unit in collaboration with branch/business unit.

Capability sets are available for information management professionals and data analytics professionals that document the key skills, knowledge and behaviours required of these professionals in [the Organisation], and others with information management and data analytics accountabilities.

People can seek additional advice/support from the Information Management and PowerBI Viva Engage communities and the Data Analytics and Insights Community of Practice on the VPS Innovation network.

Completion of Data Management Plans for significant assets is improving with support provided by the Data Management, Standards and Privacy team.

Unknown.

Strategies and programs of work have been implemented to address gaps in information management skills, capability, and capacity, with dedicated staff and ongoing projects, although some areas still face challenges in consistency and prioritisation. Information and Records Management strategy in place for current and future work to improve governance. Data Governance strategy is awaiting approval. Champions across [the Organisation] for information, data and records initiatives.

Some data capability is present in specific teams and applications, however there is no holistic program to assess and improve data capability or capacity.

Staff with specialised data skills have been appointed into dedicated data analysis roles and support the business across a variety of business needs. So, while some expertise exists in various pockets of [the Organisation], there are insufficient resources to progress all required work.

[The Organisation] recruit subject matter experts (SMEs) in specialist areas (eg: data management) to support and develop good data management, such as HR, data management.

SMEs are utilised to assist in the data requirement gathering to ensure business needs are met.

Building the foundation of an integrated [business function] platform to securely manage the data.

Incorporate Data Governance, Data Integration.

Implement data initiatives to enhance the quality delivered.

Data Management systems are secured and maintained with efforts being made to improve them and increase the value of the data collected as seen by the push for new systems such as ServiceNow and Records365.

Data is secured and teams that carry sensitive information are able to contact multiple support teams for guidance in the information handling (Specialist Teams Consulted).

Capability across the organisation has meaningful impact with limited capacity. Operating in silos, there is evidence of duplication of effort leading to competing priorities and lack of coordination required to maximise business value.

## 2.3 People: 1.3 Training, support and knowledge sharing

### From the questionnaire

Question:

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

Examples of evidence:

- The organisation has established initiatives to help build a positive data management culture and educate staff on their data management responsibilities. Staff have access to and utilise a range of internal or external data and records management courses and/or knowledge sharing tools relevant to their role.
- Training is regularly reviewed and updated to suit needs, with the results of reviews actioned and a clear escalation path documented as part of the review process.
- Formal training has been established and is regularly maintained to build and continually improve 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 and actively utilised.
- The organisation invests in upskilling staff to support data management.
- Executives use data or data insights to inform and communicate strategic decisions with staff.

### Supporting comments from participating organisations:

[Business area] have procured a data literacy roadmap, but have not had the resources for a wide implementation or rollout at this stage.

Whilst there is a degree of training and support provided this can mature and become regular. The organisation has increasing demand and interest in being data driven, however whilst this is progressing there is significant room for progression.

One respondent indicates in their team a highly collaborative approach where junior staff are actively supported to develop data and information management capabilities.

There are varied approaches to training, support and knowledge sharing across [the Organisation]: data management specialists in some Groups/Divisions attend data specific training courses as appropriate to their roles, in others, staff educate each other, or limited training is available.

There are some policies/standards available to support data use and management, but these are limited.

The Information Management SharePoint site is regularly updated to share news, key projects, policies, standards, guides, tools, and manage governance groups. Supporting information for relevant policies is also available on the intranet, and data information and literacy resources including dashboard guides for developers and consumers, turning data into information eLearning modules, and links to resources on other websites such as the Innovation Network.

Guides are available for Privacy (Impact Assessments, Breaches), Security (information classification and system security assessments), Data Access and Release, Information Governance, Data collection principles, and Data Quality.

Practical guidance is provided during the Privacy Impact Assessment (PIA) process by legal and cyber security to project proponents.

The Centre for Evaluation and Research Excellence (CERE) conducts regular training sessions including Introduction to Data Visualisation, Introduction to Evaluation, Fundamentals of Program Monitoring and Performance Measurement, and Introduction to Ethics and Approval Processes in Evaluation and Research. They also run regular drop-in evaluation clinics to help staff apply evaluation in practice and provide support for lapsing program evaluations.

The Centre for Victorian Data Linkage gives presentations to government and non-government research community on data linkage requirements in relevant forums.

LinkedIn learning has courses on data management and related subjects which are made available to all staff.

Communities of Practice create a space to learn from peers, share knowledge and resources. A list of these is available on the intranet, including Data Viz, and Power BI.

Staff are encouraged to engage with VPS Innovation network communities of practice.

An Information Management Viva Engage community is used to share tips, promote events, and request advice and assistance.

Knowledge is shared at bi-monthly Information and Data Management Reference Group.

The following eLearning modules are deployed to all staff as part of mandatory compliance training, with a refresher every two years. This training supports staff to know their obligation to manage information securely:

- Code of conduct (references using information, recordkeeping, legislative compliance).
- Security Awareness, including 6 modules: Information security obligations, You are the shield, Data security, Social engineering, email and phishing, Targeted attacks.

Annual promotion of Cyber Security Awareness Month, and Privacy Awareness Week activities and resources.

No dedicated or coordinated [Organisational] program of training exists.

The Information Management SharePoint site is regularly updated to share news, key projects, policies, standards, guides, tools, and manage governance groups. Supporting information for relevant policies is also available on the intranet, and data information and literacy resources including dashboard guides for developers and consumers, turning data into information eLearning modules, and links to resources on other websites such as the Innovation Network.

Guides are available for Privacy (Impact Assessments, Breaches), Security (information classification and system security assessments), Data Access and Release, Information Governance, Data collection principles, and Data Quality.

Practical guidance is provided during the Privacy Impact Assessment (PIA) process by legal and cyber security to project proponents.

The Centre for Evaluation and Research Excellence (CERE) conducts regular training sessions including Introduction to Data Visualisation, Introduction to Evaluation, Fundamentals of Program Monitoring and Performance Measurement, and Introduction to Ethics and Approval Processes in Evaluation and Research. They also run regular drop-in evaluation clinics to help staff apply evaluation in practice and provide support for lapsing program evaluations.

The Centre for Victorian Data Linkage gives presentations to government and non-government research community on data linkage requirements in relevant forums.

LinkedIn learning has courses on data management and related subjects which are made available to all staff. Communities of Practice create a space to learn from peers, share knowledge and resources. A list of these is available on the intranet, including Data Viz, and Power BI. Staff are encouraged to engage with VPS Innovation network communities of practice.

An Information Management Viva Engage community is used to share tips, promote events, and request advice and assistance.

Knowledge is shared at monthly reference and data governance group meetings, such as the Information and Data Management Reference Group and [business function] Data Governance Group.

The following eLearning modules are deployed to all staff as part of mandatory compliance training, with a refresher every two years. This training supports staff to know their obligation to manage information securely:

- Code of conduct (references using information, recordkeeping, legislative compliance).
- Privacy awareness.
- Security Awareness, including 6 modules: Information security obligations, You are the shield, Data security, Social engineering, email and phishing, Targeted attacks.
- At the end of August 2024, current staff members had completed the following compliance training in the past two years:
  - 86.2% ... had completed the Code of Conduct compliance training,
  - 92.3% ... had completed the Privacy Awareness compliance training, and
  - 90.7% ... had completed the Security Awareness compliance training.

Annual promotion of Cyber Security Awareness Month, and Privacy Awareness Week activities and resources.

This assessment is based on only 2 areas in [the Organisation]. Staff in Evidence and Insights manage data in line with organisational requirements and use data effectively in a manner that is commensurate to their roles. – They have a lot of new starters, so they are spending time on getting them up to scratch on policies and procedures (managed through SharePoint).

Staff that have been in the branch for some are educated and encouraged to exploit data to the fullest. They actively engage in new data management initiatives and seek better understanding of the organisation's data assets. FES is a data driven business that is implementing business processes around data. It is unclear what other business units have in place around data.

Staff have access to and utilise a range of internal or external information and records management courses and/or knowledge sharing tools relevant to their role. However, not all staff may be aware of these offerings. Mandatory training will ensure staff are kept updated on their obligations.

No [Organisation] wide training for data currently exists.

No [Organisation] wide training for staff currently exists.

Knowledge sharing are held fortnightly for an open discussion with presentation from other teams.

Eighty percent of our data sets are catalogued in the Data Governance platform.

Industry standards of Modelling and Engineering practises.

Self-training on online sites (Udemy Academy) is highly encouraged with senior management requesting all staff within Data & Digital to complete Certification on various topics (Data Vault Modelling, Databricks Foundation, SQL Analysis, ESRI Academy (for Maps)) Data is secured and teams that carry sensitive information are able to contact multiple support teams for guidance in the information handling (Specialist Teams Consulted).

Data Working Group to aid in the sharing of ideas across diverse analytics teams and share knowledge with regards to challenges and opportunities for improvement. Identified training needs and requirements enterprise wide with respect to the IM Framework and specific data roles, training program with ongoing monitoring, review and update existing training content to uplift/streamline data handling modules.



## 3 D2: Organisation

### 3.1 Organisation: 2.1 Governance

#### From the questionnaire

Question:

- To what degree is data management formally governed in your organisation?

Examples of evidence:

- An internal Governance Committee, or other formal governance structure, has been established to lead, monitor, and report on data management activities.
- The Governance Committee ensures coordination, visibility, and appropriate sponsorship of data management activities within the organisation.
- The Governance Committee is chaired by an executive-level officer, reports to the Organisation head (or a peak executive body chaired by the Organisation head) and has representation from key business areas of the organisation.
- The organisation head supports and values the work of the Governance Committee.
- Appropriate controls are in place to govern data formally and holistically across the organisation.

#### Supporting comments from participating organisations:

An executive level Data Governance Council has been established to lead and monitor the response to data governance issues, however, is still in the early stages of implementing the endorsed data governance operating model.

To the responding external agency, data governance is the responsibility of the Deputy CEO, Students and Services and reports to the agency Board Audit and Risk Committee and subsequently the full Board of the agency where appropriate.

[The Organisation] has an overall governing body that reports to its Executive Board on data and technology. This governing body is chaired by a Deputy Secretary and membership is drawn from [the Organisation's] senior executives.

[The Organisation's] Architecture Review Board assesses solution designs for systems and applications.

The governing framework includes an Information Management Policy and an Information Security Policy, which encompass data. There are some specific policies/standards in place that guide data related developments, eg Analytical Reporting Platform Design Standards.

In some cases, Groups/Divisions have established their own committees or governance frameworks to oversight their data management activities.

The ICT Subcommittee leads, monitors and reports on data management activities. Chaired by a [member of the Executive], membership includes senior management representatives across [the Organisation].

The Information and Data Management Reference Group (IDMRG), chaired by the [a senior executive staff member], includes subject matter experts from areas such as [business function] information, risk and performance, security, records, privacy and legal. It discusses and reviews key projects and initiatives, advises on strategic objectives and operational requirements, encourages development of common practices, supports knowledge transfer, and provides advice and makes recommendations to the ICT subcommittee.

The Information Management (IM) team consults and provides advice on data governance initiatives for various parts of [the Organisation], for example, Corporate Services BI system. The team is involved in all ICT projects that include data and ensure that good data management and governance processes are applied.

The National Health Data Hub (NHDH) Advisory Committee reviews and approves of data requests from government and non-government researchers for the use of the national linked health data asset.

[The Organisation's] Information Asset Governance policy aligns with the WoVG standards. Governance roles and responsibilities are defined and documented in the Information Asset Register. Formal governance plans exist for a number of critical data assets and are in development for the remainder of critical assets. Any delegation of authority is documented.

Data Management coordination responsibility in [the Organisation] requires clarification. There are not currently structures in place to support/progress DM work.

The Executive Board—operational meeting (EB) leads, monitors, and reports on IM/DM activities. Chaired by [the Head of the Public Office], membership includes senior executives from across [the Organisation] and Administrative Offices.

The Information and Data Management Reference Group (IDMRG), chaired by [a senior executive staff member] reports to the EB and includes subject matter experts from areas such as [business function] information, risk and performance, security, records, privacy and legal. It discusses and reviews key projects and initiatives, advises on strategic objectives and operational requirements, encourages development of common practices, supports knowledge transfer, and provides advice and makes recommendations to EB.

The [business function] Data Governance Group includes representatives across [the Organisation] and Administrative Offices with expert knowledge of the key [business function] data collections. New data collection proposals and changes to collections and reporting needs to be endorsed by this group.

The Information Management (IM) team consults and provides advice on data governance initiatives for various parts of [the Organisation], for example, Corporate Services BI system. The team is involved in all ICT projects that include data and ensure that good data management and governance processes are applied.

The National Health Data Hub (NHDH) Advisory Committee reviews and approves of data requests from government and non-government researchers for the use of the national linked health data asset.

[The Organisation's] Information Asset Governance policy aligns with the WoVG standards. Governance roles and responsibilities are defined and documented in the Information Asset

Register. Formal governance plans exist for a number of critical data assets and are in development for the remainder of critical assets. Any delegation of authority is documented.

There is an awareness of data management and governance in Evidence and Insights, with them actively addressing this in the EDIE data lake environment, however there is no one area that has been designated with corporate responsibility over data management/governance.

[The Organisation] has an IT Governance committee where information governance, risk, and security matters are discussed. The IM/RM strategy informs governance-related work in [the Organisation]. Work undertaken as part of the Victorian Protective Data Security Framework enhances data governance as well. [The Organisation] managers supports and values the work of the Governance Committee. Appropriate controls are in place to govern information formally and holistically across the organisation. However, need to be more consistent and bring awareness.

There is currently no internal governance data-related committee or appropriate controls to manage data holistically.

There is currently no internal governance data-related committee or internal data governance at [an Organisational] level.

Data is governed through security access models and policies around data accessibility.

Training is provided to users on how to manage access to data.

Established a Digital Transformation Committee (internal tier 1 committee) including Data and Information Management Sub-committee that strategically focuses on enterprise data and IM relating to governance/audits, risk management and compliance with organisational and government frameworks, policies and associated standards. Established several strategic projects and action plans to support the uplift of IM maturity through the IM Strategy, IM Program of Work/EDRMS implementation and IM Roadmap.

## 3.2 Organisation: 2.2 Vision and strategy

### From the questionnaire

Question:

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

Examples of evidence:

- A strategy (or strategies) for data management strategy has been developed, formally endorsed (by the executive-level representative who chairs the formal Governance Committee or higher) and adopted across the organisation. The strategy outlines the organisation's vision for the systematic approach to the management of data and is overseen by the Governance Committee.
- The Strategy adequately highlights organisation-wide data management issues, major risks, desired results, and the resource implications. Strategy development was achieved through collaboration between data management and business representatives to align to the

organisation's vision, strategic objectives, and business drivers. The strategy is aligned with other relevant strategies.

- The data management strategy is assessed for improvement on an annual basis, with improvements actioned. The initiatives of the data management strategy are resourced, funded, and actively addressed. Other strategic documents are in place in the organisation, which adequately cover data management needs and initiatives.

#### **Supporting comments from participating organisations:**

The Information Management Strategy addresses data management, particularly through the strategic approach of the development of a central data analytics platform for [the Organisation]. However more is needed to implement the identified approach, and the work is ongoing.

Whilst the digitisation strategy of the responding external statutory agency provides their vision it does not provide sufficient clarity around data management strategy.

[The Organisation] does not have a data management strategy, vision or road map.

Some Groups/Divisions have developed or are developing data management strategies and other resources (e.g. data catalogues) to meet their needs.

In other cases, projects are scoped and implemented on an as needs basis.

Examples of initiatives resourced and funded since the last review include:

- implementation of the Purview Data Catalogue
- Inclusion of new datasets into the [central data repository].

[...] [The Organisation] is still in the establishment phase. No strategy is in place.

Proposals for new data collections are required to be endorsed by the [business function] Data Governance Group.

A Data Analytics strategy has been developed.

The [business function] Data Strategy provides a roadmap for reform of the major [business function] data collections managed by [the Organisation] and the modernisation of the technologies used.

Examples of initiatives resourced and funded since the last review include:

- implementation of the Purview Data Catalogue
- Inclusion of new datasets into the [central data repository].

N/A [not applicable].

The draft Data Governance Strategy adequately highlights organisation-wide data management issues, major risks, desired results, and the resource implications. Strategy development was achieved through collaboration between information management, data and business representatives to align to the organisation's vision, strategic objectives, and business drivers. The strategy is aligned with other relevant strategies.

[The Organisation] is yet to develop a strategy or roadmap.

There is no current [Organisational] data strategy or vision.



Planned progress evident toward incorporation of predecessor agencies.

The Executive Leadership of Data and Digital shared the forward vision for the Data Engineering & Modelling for 24/25. The objectives of the vision also include metrics to measure the success of these initiatives.

A Strategy of Data Management has been developed (R365 Governance).

IM Strategy (draft) at final stages of socialisation highlights the vision covers key areas to aid the uplift of digital information and data usage and highlights the need for data to be treated as a valuable asset.

### 3.3 Organisation: 2.3 Strategic alignment

#### From the questionnaire

Question:

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

Examples of evidence:

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

#### Supporting comments from participating organisations:

Through the attempt to centralise new data analytics workloads into a single platform we are nudging [the Organisation] toward a strategic alignment on data management. However the platform is still in its infancy and there remains a great deal of complexity and fragmentation in [the Organisation's] overall approach to data management.

As with Information Management, data management especially data retention is a consideration in strategic planning (VRQA).

[The Organisation] does not have a Data Management Strategy.

Some Groups/Divisions have developed their own strategies to align with other strategic planning (eg information, risk, privacy, FOI, cyber security, information technology, procurement, or environmental management strategies).

Otherwise, integration of data management strategies and other strategic planning is ad hoc.

[The Organisational] Information Management Strategy 2021-24 is made under the Information Management Framework and is supported by information management and security policies.

The IM Strategy aligns to and supports [the Organisation's] Strategic Plan 2022-23.

[The Organisation's] Strategic Plan includes:

- effective data management and information-sharing within [the Organisation] and across government and the sector
- improve our use of data insights and promote evidence-based program and service design increase effectiveness, appropriateness and integration of technology, IT systems and information management
- increase use of evidence, evaluation, outcome measurement and data to inform planning, investment, practice and policy design.

[The Organisation's] Information Management Strategy 2021-24 is made under the Information Management Framework and is supported by information management and security policies, and the Technology Strategy.

Information Management team is involved in data and technology projects to ensure alignment with the IM Strategy.

Enterprise architecture principles guide the governance, process and practice of [the Organisation's] architecture, including building on preferred foundation platforms, enabling easier integration, sharing and re-use.

Breach of privacy and confidentiality is recognised in [the Organisation's] Risk Framework.

A summary of information privacy principles and health privacy principles are available on the intranet.

The Identity and Access Management Policy and standards state the rules [the Organisation] and its partners must follow regarding identity and access management of our systems.

... [The Organisation] is still in the establishment phase.

[The Organisation's] Information Management Strategy 2021-24 is made under the Information Management Framework and is supported by information management and security policies, and the Technology Strategy. The Strategy aligns to and supports [the Organisation's] Operational Plan.

[The Organisation's] Operational Plan includes using data, evidence and insights to develop and deliver safer, more innovative, treatments and care.

Information Management team is involved in data and technology projects to ensure alignment with the IM Strategy.

Enterprise architecture principles guide the governance, process and practice of [the Organisation's] architecture, including building on preferred foundation platforms, enabling easier integration, sharing and re-use.

Breach of privacy and confidentiality is recognised in [the Organisation's] Risk Framework.

A summary of information privacy principles and health privacy principles are available on the intranet.

The Identity and Access Management Policy and standards state the rules [the Organisation] and its partners must follow regarding identity and access management of our systems.

The Data Analytics Professional capability sets are key enablers for the IM Strategy.

N/A [not applicable].

Data management capabilities are integrated into the business through strategic planning, policy development, and project implementation. Cyber strategy and roadmap is aligned with the draft data strategy and IM/RM strategy and related policies. Business planning includes governance alignment.

There are currently no data management elements incorporated into key organisational processes and procedures nor are they aligned with other strategic planning in the organisation.

There are currently no data management elements incorporated into key organisational policies nor are they aligned with other strategic planning in the organisation.

The Executive Leadership of Data and Digital are proactively promoting [the Organisation's] Strategic Plan 2024-28 by encouraging the team to contribute the broader objective. An email is circulated to all members of team advising them of the alignment. The title of the email reflects that motto, i.e. "Aligning Our Efforts with [the Organisation's] Strategic Plan 2024-28".

Prioritising cost, ease, and timing sometimes crowds out other concerns. Progress toward One Digital Workplace is specifically included in [the Organisation's] Strategic Plan.

According to our strategic plan we work in congruence with the rest of our network, land and planning teams with the aim of supporting the broader organisation with our Information Management plans.

The IM Strategy is not explicitly mentioned within our Corporate Strategy however elements of both are extremely similar and hence build off one another.

Connect data and information systems is a core pillar of the Strategy for Digital Transformation Strategy. New IM Strategy (draft) at final stages of socialisation across multiple business areas.

### **3.4 Organisation: 2.4 Management, advocacy and leadership**

#### **From the questionnaire**

Question:

- Do all levels of management actively support data management in your organisation?
- Is there executive-level representation and advocacy for data management initiatives?

Examples of evidence:

- The organisation has appointed an executive level data management position, such as Chief Data Officer (or equivalent).
- Data management interests and issues are represented and advocated for at the executive level and are given appropriate consideration.

- Data management policies and practices are actively supported and adopted by Senior Management and Middle Management.
- Leadership understands data management issues and practices and seek additional specialist data when needed.

### **Supporting comments from participating organisations:**

An executive level [Committee] provides formal governance, and leads, monitors and reports on information and data management activities. The [Committee] has representation from across [the Organisation], and reports to the Executive Board. The Chief Information Officer is the executive director of [the business area], and able to advocate for information management and data management initiatives as required.

There is representation and advocacy of data management at executive level in some Groups/Divisions, but it isn't consistent across [the Organisation].

[The Organisation] has a Chief Information Officer.

[The Organisation's] governing body for data and technology acts on behalf of its Executive Board.

The Director, Strategy, Architecture and Planning, [business division] represents [the Organisation] on the WoVG Information Management Group and the WOVG CDO Leadership Group.

The Director, Cybersecurity and Assurance, [business division] represents [the Organisation] on the WOVG Cyber Security Leadership Group.

The Information and Data Management Reference Group advises on strategic objectives and operational requirements, supports knowledge transfer, and provides advice and makes recommendations to the EB. Membership includes subject matter experts from areas such as [business function] information, risk and performance, security, records, privacy and legal, and is chaired by the Director, Strategy, Architecture and Planning.

Information asset governance policies are reviewed regularly to ensure [the Organisation] appropriately and consistently manages its data and information across their lifecycle, particularly with regards to protecting the privacy of individuals, whilst maximising the benefit that can be derived through appropriate use of data within its custody, including formal approval and documentation of delegation of authority to assure data are released appropriately by authorised areas.

Privacy Impact Assessments (PIA) are a key document required at [the Organisation's] Project Initiative Assessment Group (PIAG). The Privacy and Legal Compliance Team advises and supports threshold privacy assessments to identify key privacy risks; and privacy impact assessments in summary form for less complex matters or where project timeframes require an expedited review, or PIAs in the traditional form.

Cyber security risks are reported in [the Organisation's] strategic risks report on a quarterly basis with KPI with the Joint Cyber Security Steering Committee (JCSSC) providing oversight of the Cyber security program. Cyber security risk is now listed as a Tier 1 risk for [the Organisation].

There is strong awareness of the importance of data in specific areas.

The [business function] Data Governance Group was established in December 2019 to make decisions regarding the alignment of [business function] data projects and activities with [the Organisation's] Information Management Strategy. It provides advice and assistance to business areas regarding the management of [business function] data and information, and provides advice and makes recommendations to the EB. Membership includes representatives across [the Organisation] and Administrative Offices with expert knowledge of the key [business function] data collections and is chaired by the Director, Strategy, Architecture and Planning.

The Director, Strategy, Architecture and Planning, [business division] represents [the Organisation] on the WoVG Information Management Group and the WOVG CDO Leadership Group.

The Director, Cybersecurity and Assurance, [business division] represents [the Organisation] on the WOVG Cyber Security Leadership Group.

The Information and Data Management Reference Group advises on strategic objectives and operational requirements, supports knowledge transfer, and provides advice and makes recommendations to the EB. Membership includes subject matter experts from areas such as [business function] information, risk and performance, security, records, privacy and legal, and is chaired by the Director, Strategy, Architecture and Planning.

Information asset governance policies are reviewed regularly to ensure [the Organisation] appropriately and consistently manages its data and information across their lifecycle, particularly with regards to protecting the privacy of individuals, whilst maximising the benefit that can be derived through appropriate use of data within its custody, including formal approval and documentation of delegation of authority to assure data are released appropriately by authorised areas.

Privacy Impact Assessments (PIA) are a key document required at [the Organisation's] Project Initiative Assessment Group (PIAG). The Privacy and Legal Compliance Team advises and supports threshold privacy assessments to identify key privacy risks; and privacy impact assessments in summary form for less complex matters or where project timeframes require an expedited review, or PIAs in the traditional form.

Compromise of information is recognised in [the Organisation's] Risk Framework within the 'Information, technology and security' risk consequence category which was most recently updated in September 2024.

Cyber security risks are reported in [the Organisation's] strategic risks report on a quarterly basis with KPI with the Joint Cyber Security Steering Committee (JCSSC) providing oversight of the Cyber security program. Cyber security risk is now listed as a Tier 1 risk for [the Organisation].

While we have no Chief Data Officer or area responsible for corporate data management/governance, we do have a Digital and Data Leadership Committee.

Senior and Middle Management actively support and adopt data management policies and practices. [The Organisation] has a CDO equivalent.

The importance of data is recognised as being key to completing reporting obligations and to gain insights into programs and activities. Leaders are aware that data and data analysis is vital to support the definition and delivery of services and programs.

There is strong awareness re: importance of data in specific areas, but there is no executive level position responsible for internal data governance and data management best practice.

There is Executive representation, particularly in relation to Information Security.

The Data Modelling & Engineering encouraging staff members to attend various professional engagements for self-development:

- Leadership Training
- Mentor Program for Training (SQL for Analysis, Databricks)
- Conference Presentations
- Training through Udemy Academy
- Centralised Data structure.

Dedicated Chief Digital Officer, Chief Information Security Officer, Agency Security Advisor and Group Manager, Intelligence, Investigation & Analytics. [A senior executive member] chairs the DTC and EDRMS PCB (tier 1 committees).

### **3.5 Organisation: 2.5 Audit and compliance**

#### **From the questionnaire**

Question:

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

Examples of evidence:

- The organisation has an internal audit process/program in place to work towards achieving compliance against data management relevant legislation, policies, and standards (such as those issued by Public Record Office Victoria and Office of the Victorian Information Commissioner).
- Data management compliance requirements are known, communicated, and applied within the organisation. Documents or processes are in place to help staff understand how to apply relevant legislation or policies to their collection, analyses, and use of data. Corrective actions have been implemented to address causes of non-compliance. Opportunities to improve data management compliance are explored and implemented.

#### **Supporting comments from participating organisations:**

More remains to be done to achieve full compliance, however activities such as the OVIC attestation process, this IM3 reporting, internal and external audit functions and the responses to them through executive level committees such as the Data Governance Council, all suggest that initiatives are operating to a reasonable level.

Data management while management and monitored by the information services team requires more maturity among the wider organisation staff.

There is limited auditing of data management practices. It is carried out on a needs or request basis.

The records management team is engaged when needed.

[The Organisation] audits its data security related activities annually through the OVIC Privacy and Data Protection Act attestation process.

[The Organisation's] Audit and Risk Management Committee provides advice on [the Organisation's] risk management framework and controls and verifies compliance with the requirements of the Victorian Government Risk Management Framework to support risk management attestation.

Risks identified in the framework with IM audit and compliance considerations:

- breach of privacy and confidentiality
- legal, regulatory and compliance
- cyber security incidents and Victorian Protective Data Security Standards (VPDSS).

A dedicated, expert Privacy unit comprised of legal SMEs provide oversight, guidance, and enforcement of [the Organisation's] privacy obligations.

IM related policies and supporting documents are in place, such as the 'Managing privacy incident guide' to assist staff to respond to privacy incidents and the 'Data Access and Release Guide'.

An accreditation process for units that routinely share data has been instituted and requires units to undergo an assessment of their data management processes and training.

In many cases, external data releases must be under a data sharing agreement that requires the recipient to manage data according to legislation and Information Privacy and or Health Information Privacy Principles.

Attestation to the Office of the Victoria Information Commissioner (OVIC) for VPDSS every 2 years. An attestation for [the Organisation] was submitted to OVIC at the end of August 2024.

New projects that involve the collection, use or disclosure of personally identifying information must be formally assessed for privacy compliance and this may be in the form of a Threshold Privacy Assessment, or written Privacy Impact Assessment (PIA) whether in summary or traditional form, which assesses the project's compliance with key privacy legislation, information security requirements and (as relevant) record keeping obligations.

Use of Protective Markings is standard practice across [the Organisation]. Monitoring focuses on trends such as emails marked as protected being sent outside [the Organisation] and followed up with education.

[The Organisation's] strategic and annual internal audit program considers information technology risks through penetration tests mimicking threat actors (targeted at legacy systems and applications hosted in the MS Azure environment), cyclical review of controls identified in the ACSC's Essential 8 as critical risk mitigations and ad hoc reviews requested by management and / or Audit and Risk Management Committee.

[The Organisation] participates in yearly reviews and audits conducted by VAGO and external auditors that assess the disaster recovery (DR) preparedness and ongoing DR testing of critical and financial IT systems.

VAGO have initiated a Critical Data Assets audit. There is no other audit and compliance program in place for DM though.

[The Organisation's] Audit and Risk Management Committee provides advice on [the Organisation's] risk management framework and controls and verifies compliance with the requirements of the Victorian Government Risk Management Framework to support risk management attestation.

Risks identified in the framework with IM audit and compliance considerations:

- breach of privacy and confidentiality
- legal, regulatory and compliance
- cyber security incidents and Victorian Protective Data Security Standards (VPDSS).

A dedicated, expert Privacy unit comprised of legal SME's provide oversight, guidance, and enforcement of [the Organisation's] privacy obligations.

IM related policies and supporting documents are in place, such as the 'Managing privacy incident guide' to assist staff to respond to privacy incidents and the 'Data Access and Release Guide'.

An accreditation process for units that routinely share data has been instituted and requires units to undergo an assessment of their data management processes and training.

In many cases, external data releases must be under a data sharing agreement that requires the recipient to manage data according to legislation and Information Privacy and or Health Information Privacy Principles.

Attestation to the Office of the Victoria Information Commissioner (OVIC) for VPDSS every 2 years. An attestation for [the Organisation] was submitted to OVIC at the end of August 2024.

New projects that involve the collection, use or disclosure of personally identifying information must be formally assessed for privacy compliance and this may be in the form of a Threshold Privacy Assessment, or written Privacy Impact Assessment (PIA) whether in summary or traditional form, which assesses the project's compliance with key privacy legislation, information security requirements and (as relevant) record keeping obligations.

Use of Protective Markings is standard practice across [the Organisation]. Monitoring focuses on trends such as emails marked as protected being sent outside [the Organisation] and followed up with education.

[The Organisation's] strategic and annual internal audit program considers information technology risks through penetration tests mimicking threat actors (targeted at legacy systems and applications hosted in the MS Azure environment), cyclical review of controls identified in the ACSC's Essential 8 as critical risk mitigations and ad hoc reviews requested by management and / or Audit and Risk Management Committee.

[The Organisation] participates in yearly reviews and audits conducted by VAGO and external auditors that assess the disaster recovery (DR) preparedness and ongoing DR testing of critical and financial IT systems.

N/A [not applicable].

[The Organisation] has an internal audit process/program in place to work towards achieving compliance against information and data management relevant legislation, policies, and standards (such as those issued by Public Record Office Victoria and Office of the Victorian Information Commissioner). Information and data assets are reviewed and the register enhanced this year to improve visibility.

There is no audit and compliance program in place for data.

There is no audit and compliance program in place for DM.

FOI compliance requirements largely met. Victorian Protective Data Security Standards maturity assessed at Basic and Core levels. Internal audit program addresses matters related to Information Management, e.g., Guidelines for notification to OVIC of (Privacy and) Data breaches.

Cyber Security and Data Governance assisting in developing solution that are aligned to policy.

Initial audit from VAGO allowed us to address some data quality metrics & info.

Organisation is regularly audited by 3rd party.

Data Management is more maintained and stricter than information management processes as the data management is done by specialised teams.

All requirements are upheld within the organisation and teams are available for consultation to avoid non-compliance.

Large organisation resulting in struggles to spread proper processes.

Internal audit completed by a third-party to assess the current state maturity of our Data Governance Framework and the design of supporting processes to manage data enterprise wide. This audit was assessed against the Victorian IM Framework, Victorian Protective Data Security Standard and the Privacy and Data Protection Act 2014. Key focus was on accountability, roles and responsibilities, data ownership, data management, data use and data sharing.

## 4 D3: Lifecycle and Quality

### 4.1 Lifecycle and quality: 3.1 Asset management

#### From the questionnaire

Question:

- How well does the organisation identify, manage, monitor, and utilise their significant data assets?
- Have data management roles and responsibilities been defined and applied in the organisation to properly manage data assets?

Examples of evidence:

- The organisation's significant data assets (i.e., discrete collections of data that is recognised as valuable) and critical data assets (i.e., subsets of significant data assets that are considered high value/high risk or vital) have been identified. A data catalogue has been established, maintained to document at minimum, the organisation's significant data assets and are demonstrably benefiting the organisation.
- The organisation uses a central, enterprise-wide data catalogue, inventory and/or asset register that has well-defined processes for data classification. The organisation has consistent definitions, metadata and governance to support the data inventory/asset register. The data inventory/asset register is updated and maintained regularly and consistently, and supported by appropriate tools and services (data catalogue).
- A custodianship model is in place so that assets have an assigned owner and custodian (or equivalent) who are aware of and undertake their role and responsibilities in relation to the data assets assigned. The custodianship model supports work with data users to actively maintain assets and improve the accessibility, usability and sharing of data as required. Users are aware of the data catalogue and their responsibilities in relation to it, can assess if assets are fit for their intended purpose, and locate and use the relevant asset when needed, if access is approved.
- Data custodians and data stewards are identified for key data assets and have clearly defined roles, aligned to legislation and/or policies. Data custodian and data steward roles are linked to performance documentation and expectations. Data custodians and data stewards have clearly defined expectations and accountabilities regarding the quality, treatment, access, and group's use of the data.

#### Supporting comments from participating organisations:

An Information Asset Register has been implemented, though not widely used. There are plans underway to transition to a Data Catalogue solution for better identification of information and data assets and their responsible parties.

The responding external agency's data assets are owned by the Deputy CEO, Students and Services who has expertise in information management.

There is some awareness of the need for data asset management, but it is not consistent across the organisation. As a result, the level of maturity is variable.

Some Groups/Divisions have developed data custodianship models so that assets have an assigned owner and custodian who maintain their assets and improve the accessibility, usability and sharing of data as required, or have data specialists who actively manage their major datasets.

In other cases, some data may be formally managed, but others have less oversight, or informal processes may be applied by individual staff.

[The Organisation's] Cyber Security Program has increased the visibility and importance of managing data assets by developing an Information Asset Register.

Information asset governance roles are defined, including accountability and responsibility for data including Discoverability, Access and Release, Usability, Quality, Security, and Privacy.

An accreditation process for units that routinely share data requires units to undergo an assessment of their data management processes and training.

A Delegation Schedule has been created and work is underway to document and formalise delegations of Custodian authority to other parties.

A Data Management Plan template is available for staff to describe how assets are managed and governed to improve transparency, knowledge sharing and governance. Usage of the template is increasing.

[The Organisation's] Information Asset Register is central to its efforts to make information easy to find, access and use, and is available to all staff within [the Organisation] via the OurInformation SharePoint. It includes the Protective Marking and Business Impact Levels, and names of governance role holders.

The Records Management Unit has created a new assessment tool to manage records in a business system due for decommissioning to compliantly manage the information stored and to support analysis, appraisal, and disposal activities.

The [central data repository] is a secure, managed central location where [Organisation] datasets are stored, discovered, used and shared. It provides easier access to data across [the Organisation], by decoupling the operational systems, environments and integration from the sharing of the data from these systems. It also stores commonly used enterprise reference or master data, or curated datasets. Currently 76 datasets are available.

The [resources] and [linked datasets].

The [secure virtual environment] is a secure data access environment that enables dissemination of linked data within a secure-based cloud environment, with analysis undertake via a dedicated Virtual Machine (VM).

[The Organisation's] IAR has been developed.

Information asset governance roles are defined, including accountability and responsibility for data including Discoverability, Access and Release, Usability, Quality, Security, and Privacy.

An accreditation process for units that routinely share data requires units to undergo an assessment of their data management processes and training.

A Delegation Schedule has been created and work is underway to document and formalise delegations of Custodian authority to other parties.

A Data Management Plan template is available for staff to describe how assets are managed and governed to improve transparency, knowledge sharing and governance. Usage of the template is increasing.

[The Organisation's] Information Asset Register is central to its efforts to make information easy to find, access and use, and is available to all staff within [the Organisation] via the OurInformation SharePoint. It includes the Protective Marking and Business Impact Levels, and names of governance role holders.

The Records Management Unit has created a new assessment tool to manage records in a business system due for decommissioning to compliantly manage the information stored and to support analysis, appraisal, and disposal activities.

Audit programs relating to the data quality (of information provided by the sector) are in place for limited number of [business function] data collections.

The [business function] Data Strategy provides a 3-5 year roadmap for reform of [business function] data collection and modernisation of the technologies used. It describes the desired future state of [business function] data in [the Organisation] and the activities required to achieve it. The Strategy aligns with and supports [the Organisation's] IM Strategy.

The [central data repository] is a secure, managed central location where [Organisation] datasets are stored, discovered, used and shared. It provides easier access to data across [the Organisation], by decoupling the operational systems, environments and integration from the sharing of the data from these systems. It also stores commonly used enterprise reference or master data, or curated datasets. Currently 76 datasets are available.

The [resources] and [linked datasets].

The [secure virtual environment] is a secure data access environment that enables dissemination of linked data within a secure-based cloud environment, with analysis undertake via a dedicated Virtual Machine (VM).

The higher mark was attributed to [business unit 1] which has Data custodians and Data stewards clearly defined for [the Organisation's] data with clear expectations and accountabilities regarding the quality, treatment, access, and group's use of the data. [Business unit 2 and business unit 3] data are newer additions to the branch and these roles and responsibilities need to be revisited. Next Gen and other data collections do not. [Business unit 1] are highly proactive, whilst the remainder of [the Organisation] is not at the same level.

[The Organisation's] critical and significant information assets have been identified and recorded in the Information Asset Register (IAR). The IAR is reviewed annually together with information owners, additionally a new project is progressing to improve visibility, discoverability and end user experience for [the Organisation] of its information assets. Data assets are captured in the same register which identifies significant, critical and valuable assets.

While data in systems has been included in the Information Asset Register (IAR), there has been no specific work to identify and include data sets.

While data in systems has been included in the Information Asset Register (IAR), there has been no specific work to identify and include data sets.

[The Organisation] has continued with the implementation of the Information Asset Register and the Custodianship model exists, based on the Organisation structure.

Data is stored in unique repositories within cloud-based environments with sensitive/non-sensitive layer based on security assessments.

Documentation of data attributes is catalogued in the Data Governance platform for wider access with access managed.

Data management roles and responsibilities have been defined, and assets are centrally located in unique.

Following completion of an information review in 2023, we recorded all significant/critical and non-significant/critical Information Assets (IAs) onto the IAR. All new IAs are captured during the end-to-end delivery framework via an Information and Security Assessment for all new and existing upgraded IAs which is triggered for an update at least annually.

## 4.2 Lifecycle and quality: 3.2 Policies and procedures

### From the questionnaire

Question:

- Does the organisation have fully developed and implemented data management policies that align to relevant legislation and standards?
- Are these policies supported by documented procedures?

Examples of evidence:

- The organisation has established data management policies that align to relevant legislation and standards (such as those issued by Public Record Office Victoria and Office of the Victorian Information Commissioner).
- The policies have been approved and endorsed by the Secretary or an executive level board/officer and are actively supported by all levels of management.
- The policies are actively communicated and available to all staff, who are aware of and act in accordance with the directives specified within them.
- Data management 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, with improvements actioned.
- Breaches of policy are actively addressed and rectified, with a clear escalation path documented as part of the process.

### **Supporting comments from participating organisations:**

[The Organisation] is a little less mature in terms of data management policies. There are pockets of good practice, but also significant gaps in terms of gaining access to definitive advice or support.

One respondent responds that they document all of their infrastructure constructed for analysing and reporting on [business] workforce metrics.

The responding external agency adheres to [the Organisation's] data management requirements and overlay this with additional requirements for users of VRQA systems.

[The Organisation] does not have policies relating to data management. It has an Information Management Policy and a Records Management Policy aligned to relevant legislation and standards. These are complemented by an Information Security Policy.

These policies are published on [the Organisation's] intranet and are reviewed annually.

Some Groups/Divisions have developed their own strategies, plans, procedures and frameworks under [the Organisation's] policy umbrella to support their local needs. In other cases, informal data management practices are in place or others are reliant on a small group of data professionals who apply their best efforts for responsible data management.

The Data Access and Release Policy, Data Quality Policy and associated documents align with Victorian Public Service Information Management Policy, Governance Standards and Guidelines, and are available to all staff via the Intranet and SharePoint. These have been recently updated. The Information Asset Governance Policy, and associated documents align with Victorian Public Service Information Management Policy, Governance Standards and Guidelines, and are available to all staff via the Intranet and SharePoint. [The Organisation's] documents are currently under review as a part of a regular review cycle.

Data requests are subject to a range of robust processes to ensure compliance with the Privacy and Data Protection Act and Health Records Act. This may include approval by data custodians for use of the data, and where required, development of a Privacy Impact Assessment, the completion of an Information Security Classification, and approval by an accredited Human Research Ethics Committee.

All external users must complete a Deed of Acknowledgment and Confidentiality outlining the conditions of access to the data (with signatures from all recipients of the data and from the organisation legally responsible for the project).

The Privacy Policy and framework align with OVIC's recommendations and are reviewed and tested in PIAs conducted for significant new projects.

Protective Markings have been rolled-out in line with the Victorian Protective Data Security Standards (VPDSS).

[The Organisation's] Information Risk Register incorporates Cyber Security Risk. The register is used as an input to [the Organisation's] VPDSS compliance review.

[The Organisation] has developed an Information Management Policy and an Information Security Policy. Information Management Policy provides high level governance for information and data. No data-specific policies/procedures in place, nor planned at the moment.

The Data Access and Release Policy, Data Quality Policy and associated documents align with Victorian Public Service Information Management Policy, Governance Standards and Guidelines, and are available to all staff via the Intranet and SharePoint. These have been recently updated. The Information Asset Governance Policy, and associated documents align with Victorian Public Service Information Management Policy, Governance Standards and Guidelines, and are available to all staff via the Intranet and SharePoint. [The Organisation's] documents are currently under review as a part of a regular review cycle.

Data requests are subject to a range of robust processes to ensure compliance with the Privacy and Data Protection Act and Health Records Act. This may include approval by data custodians for use of the data, and where required, development of a Privacy Impact Assessment, the completion of an Information Security Classification, and approval by an accredited Human Research Ethics Committee.

All external users must complete a Deed of Acknowledgment and Confidentiality outlining the conditions of access to the data (with signatures from all recipients of the data and from the organisation legally responsible for the project).

The Privacy Policy and framework align with OVIC's recommendations and are reviewed and tested in PIAs conducted for significant new projects.

Protective Markings have been rolled-out in line with the Victorian Protective Data Security Standards (VPDSS).

[The Organisation's] Information Risk Register incorporates Cyber Security Risk. The register is used as an input to [the Organisation's] VPDSS compliance review.

Detailed procedures and criteria support management (including change management) of the key [business function] data collections.

Evidence and Insights and NextGen are both in the process of implementing data management in accordance with legislative requirements.

Policies and procedures align with OVIC and PROV.

Data management processes are embedded in particular teams, but no [Organisation] level data management policies and procedures exist.

[The Organisation's] Information Management Policy provides high level governance for information and data. No data-specific policies/procedures in place for data specifically, nor planned at the moment.

[The Organisation] has various policies, procedures and guides available in the Corporate Policy Hub and referenced throughout the intranet.

[The Organisation] actively participates in data and release, self-assessments, and reviews Business Impact Levels to ensure the correct level of protection is applied to data.

MOUs and IPAs are in place across [the Organisation] however awareness and compliance may not be consistent across the business units.

Some longstanding arrangements may not be able to demonstrate up-to-date assurance that compliance and risk have been assessed.

Work is underway to uplift systems and ensure legislative requirements are met at a higher rate (for example Records Management Systems).

Completed a refresh of existing procedures and guides, launched the Information and Records Management Hub to align with best practice and excellence across the organisation, draft IM Policy progressing for approval, final stages of agency specific RDA review and ongoing feedback relating to the review of PROS 07/01 and other PROV standards.

## 4.3 Lifecycle and quality: 3.3 Meeting business and user needs

### From the questionnaire

Question:

- Is data meeting the needs of the business and its users in terms of strategic importance, quality, and accountability?

Examples of evidence:

- The organisation has established and implemented processes and/or a program to address data quality issues (ensuring data is accurate, unbiased, consistent, complete, clear, explainable, and current).
- The needs of the business are assessed routinely to determine whether the right data are being captured at the right points of the process and are accessed and used by the right people at the right time to achieve the strategic plans of the business.
- An analysis of data assets is regularly conducted to determine data is meeting business needs, accountability requirements and community expectations. The results are actioned with a clear escalation path for high-risk issues in place.
- Data quality statements have been developed and maintained for at least the significant (including critical) data assets.
- Remediation processes are in place to address data quality issues, with a clear and documented escalation path as part of the process, and remediation actions required prioritised and addressed.
- Overall, data are demonstrably fit for purpose and/or can be tailored to meet business needs within an appropriate timeframe.
- There are clear practices of collaboration between data analytics leads, data producers, and custodians to ensure proper data usage.
- Automated capabilities reduce manual cleansing steps and support streamlined maintenance of data assets (e.g., data quality, profiling, cleansing tools).

### Supporting comments from participating organisations:

An information/data quality framework has been defined, though yet to be fully implemented and approved (pending Data Governance Council review and endorsement). The need to align information and data requirements to business and user needs is widely recognised, though more needs to be done to make this a reality.

Data needs are well addressed, however there is a current focus on improving data quality.

In an environment of limited resourcing and an entrenched teacher workforce crisis, there will always be limitations to the extent to which data can provide comprehensive insights for resolving economy-wide challenges.

There is no organisation wide quality and availability program.

Locally established processes, systems and/or programs are being implemented in Groups/Divisions to meet their needs for data quality, although this is not consistent across [the Organisation].

The [central data repository] enables better data access and supports the management needs of [the Organisation]. New datasets are periodically added to the [central data repository].

Purview data catalogue intends to information to support data use.

[Organisational] Condition of Release in accordance with business and users' needs.

The [resources] and [linked datasets] to facilitate linkage of [Organisational] datasets for the research community seeking de-identified linked data.

...[U]sers are currently using separate systems and therefore different processes/practices. Visibility across [the Organisation] is limited and difficult to assess at this stage. [The Organisation] is engaged with identifying data, further work is required to assess its.

The [central data repository] enables better data access and supports the management needs of [the Organisation]. New datasets are periodically added to the [central data repository].

Purview data catalogue intends to information to support data use.

Key ... data collections are assessed annually to determine if the data is meeting business needs.

Regular compliance reports describing data completeness are provided for users of the key ... data collections.

A small number of ... Data collections provide a data quality statement in the affiliated user manual.

[Business Function] Data Strategy components implemented to support data collections that are fit for purpose.

Data Hub procedures and templates to assist with data release in accordance with privacy requirements.

[Organisational] Condition of Release in accordance with business and users' needs.

The [resources] and [linked datasets] to facilitate linkage of [Organisational] datasets for the research community seeking de-identified linked data.

For context this part of the assessment only covers 2 areas of [the Organisation]. [Business unit] have fully automated data storage, reporting and management through a secure service AWS and use many statistical tools to automate workflows (for example Tableau, Python, SQL, Power BI).

Official statistics are released publicly on the website. [Business unit 1] and [business unit 2] data are newer additions to the branch and incorporation of these data into AWS is currently being worked on. Next Gen have had a successful debtor merge activities and a reduction in overall debtor identities, and an elimination of business process backlogs. Other business units within [the

Organisation] that collect and store data were not included in this assessment as we operate on a devolved model, and do not have the resources to have extended to them.

The needs of the business are assessed routinely to determine whether the right information is being captured at the right points of the process and are accessed and used by the right people at the right time to achieve the strategic plans of the business.

Specific data products (dashboards etc) are developed and refined to the business to ensure they meet business needs. Specialised and skilled data analysts undertake work to ensure data is fit for purpose/analysis. There is currently no broader program to assess and monitor data to ensure it meets users needs i.e. there are currently no data quality statements.

Specific data products (dashboards etc) are developed and refined to the business to ensure they meet business needs. Specialised and skilled data analysts undertake work to ensure data is fit for purpose/analysis. There is currently no broader program to assess and monitor data to ensure it meets users needs i.e. there are currently no data quality statements.

Work is underway to ensure data access meets strategic need but is not yet applied consistently across [the Organisation].

Organisational attitude towards data collection and management is overall positive.

Data collection quality has been challenging but the majority of the time data has been captured well enough to assist when searching.

Processes are introduced to ensure the data quality (accuracy, completeness, consistency and current), especially with new applications.

Unit testing of the processed data is undertaken prior to the release of any modules.

Draft IM Strategy, IM Program of Work and IM Roadmap 2024-2026, draft IM and Data Quality Framework, established a centralised Information and Records Management Hub to align with best practice and excellence across the organisation and mature IAR. Currently establishing Data and Analytics Working Group representing business and technical teams required to regularly review data management practices and initiatives against policies.

## **4.4 Lifecycle and quality: 3.4 Accessibility, discoverability, and availability**

### **From the questionnaire**

Question:

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

Examples of evidence:

- An organisation-wide inventory and/or data catalogue of its data assets that is accessible to internal and external users has been developed and used by staff.
- Data are collected and stored with access and discoverability in mind. Definitions and standards are used to increase the findability of data. Sufficient metadata is provided to

correctly identify and locate data. Standard vocabulary and automated tools are used where applicable. Access to controlled data sources have been defined and implemented. Procedures have been implemented for data capture, the application of metadata, data access, storage, and retrieval.

- The organisation's data request and data access processes including security controls are reviewed and measured for continuous improvement. The organisation's Data Strategy includes the inventory and/or data catalogue inventory and/or metadata management, which is reviewed and measured for continuous improvement.
- The organisation can establish standards for metadata and provide oversight and advice to others. The organisation maintains knowledge of metadata best practice, including standards and applications. The organisation can use a range of tools for storing and working with metadata. The organisation keeps metadata refreshed and updated and can repair items that are incorrect or out of date.

### **Supporting comments from participating organisations:**

A number of these applications have been completed and implemented, including the M365 migration to the new [Organisational] intranet, and the information asset register. Procurement of a data catalogue solution is also in planning stages.

In an environment of limited resourcing and an entrenched teacher workforce crisis, there will always be limitations to the extent to which data can provide comprehensive insights for resolving economy-wide challenges.

The responding external agency has begun work to not only make more data available but also to provide mapping and reference data to make this data more usable. This is however in its infancy and there is more progress to be made.

There are activities in place to support data accessibility, discoverability and availability. but they aren't consistent across [the Organisation].

There is no centralised repository which holds [the Organisation's] data.

Some Groups are implementing data catalogues and data repositories. In other cases, data is held in systems owned/managed by third party providers.

Lack of interoperability between platforms and security policies may impact data availability.

Data are released to DataVic where appropriate, for example annual report data.

The [central data repository] is a secure, managed, central location where [Organisation] datasets are stored, discovered, used and shared. It can also store commonly used enterprise reference or master data, or curated datasets. Access to data is managed to ensure that data and information are shared or protected as appropriate.

The Information Asset Register is available on the OurInformation SharePoint site to improve discoverability. This provides Custodians with a straightforward way to register and maintain their metadata, which in turn assists other staff to discover information sources within [the Organisation].

The Purview Data Catalogue has been implemented.

The Data Access and Release Policy and supporting materials have been reviewed recently. These support staff to ensure that access and release of data held by [the Organisation's] complies with the relevant legislative requirements to ensure that the rights of the individual are upheld, and information is released only for appropriate uses. Relevant legislation is applied when considering what data to share, under which circumstances and with what conditions.

The Intranets Plus project delivered significant improvements to search and discovery across [the Organisation's] M365 tenancy and integration of the intranets search with [the Organisation's] instance of OurService.

The [resources] and [linked datasets] to facilitate linkage of [Organisational] datasets for the research community seeking de-identified linked data.

[...] [U]sers are currently using separate repositories and therefore different processes/practices. Accessibility, discoverability, etc. across [the Organisation] is limited and difficult to assess at this stage.

Data are released to the public via [Organisation] websites and DataVic where appropriate.

The [central data repository] is a secure, managed, central location where [the Organisation] datasets are stored, discovered, used and shared. It can also store commonly used enterprise reference or master data, or curated datasets. Access to data is managed to ensure that data and information are shared or protected as appropriate.

Data cubes are available to authorised [Organisation] staff.

Data and reporting is tailored to the intended audience ...

The Information Asset Register is available on the OurInformation SharePoint site to improve discoverability. This provides Custodians with a straightforward way to register and maintain their metadata, which in turn assists other staff to discover information sources within [the Organisation].

The Purview Data Catalogue has been implemented.

The Data Access and Release Policy and supporting materials have been reviewed recently. These support staff to ensure that access and release of data held by [the Organisation] complies with the relevant legislative requirements to ensure that the rights of the individual are upheld, and information is released only for appropriate uses. Relevant legislation is applied when considering what data to share, under which circumstances and with what conditions.

The Intranets Plus project delivered significant improvements to search and discovery across [the Organisation's] M365 tenancy and integration of the intranets search with [the Organisation's] instance of OurService.

The [resources] and [linked datasets] to facilitate linkage of [Organisational] datasets for the research community seeking de-identified linked data.

The online Hub data request.

For context this assessment was only carries out in 2 areas. [Business Unit] have CSA output datasets in the Victorian Data Directory. They also have fully automated tools and reporting

processes that support data accessibility. Next Gen are not as far progressed and the remainder of areas within [the Organisation] that capture, and store data were excluded.

IAR is enhanced to improve visibility of assets. As part of manage-in-place, naming conventions guidance was promoted which led to an increase in awareness. Records365 has ability to search and captures metadata.

Processes are in place to manage the access to data and it's outputs to ensure it remains secure and accessible to those who need it, especially in the areas where sensitive data is being handled. There is currently no [Organisation] wide data catalogue. There is currently no guidance on metadata best practice.

There is currently no [Organisation] wide data catalogue. However, processes are in place to manage the access to data and it's outputs to ensure it remains secure and accessible to those who need it, especially in the areas where sensitive data is being handled. There is currently no [Organisation] wide data catalogue.

A Data & Digital Service Catalogue has been developed and is maintained within [the Organisation].

Various [Organisational] Policies. Strategies and guidelines govern and support the accessibility, discoverability and availability of data, including Data Release, Data Sharing and Information Security Policies and the Technology, Data and Cyber Strategy.

Security controls are in place aligning our initiatives and actions to the VPDSF and OVIC and access to data repositories can be granted with appropriate approval mechanisms in place.

Key data for settled business purposes is available and usable within the various systems.

While this information is available on [the Organisation's] intranet there is a belief that staff's knowledge of, and use, is not consistent across [the Organisation].

Operational data requests and data access processes including security controls are reviewed continuously and measured for continuous improvement across data platforms. The internal Information Asset Register provides a foundational view to identify data assets and ownership.

Clearly defined business process to request access to data in core platforms has been established in ServiceNow aligned to Role Based Access Controls.

## 4.5 Lifecycle and quality: 3.5 Data use and reuse

### From the questionnaire

Question:

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

Examples of evidence:

- Organisation standards/procedures have been introduced to facilitate consistent data collection, description, and organisation, and to prevent duplication.



- Digital continuity strategies are in place. Data assets are shared and reused across the organisation and with external stakeholders in accordance with the original purpose of collection, privacy legislation, and other relevant regulation.
- The organisation applies appropriate licences and quality statements when sharing data to ensure it remains fit for purpose and in line with privacy and other regulations. Where appropriate, and in accordance with relevant legislation, data are released to the public.
- Custodians work with data users to support the usability of data in accordance with the original purpose of collection and relevant legislation.
- The organisation can leverage their data for business intelligence and analytics. Data exchanges occur using standard interfaces and formats and in line with relevant legislation. Custodians have documented Data Provenance; referring to the data's lifecycle, including its origins, any transformations it undergoes, and how it's used.
- Retention periods are assigned in accordance with current and authorised Standards, reviewed, and disposal actions managed in accordance with a lawful, current and executive approved disposal program.

### **Supporting comments from participating organisations:**

An Information Sharing Standard has been produced, approved and published on [the Organisation] intranet. The Information Asset Register also facilitates the sharing of information and data - although both of these are under-utilised.

Use of tools such as Power BI are in its infancy however there is a greater use of data for regular reporting including data cleansing and dashboard use in some business areas.

A key condition of our data sharing agreements with stakeholders is that data analyses are not re-used where there is a risk of identifying individual staff members. Beyond this, however, the clarity and presentation of our insights mean that general themes and findings remain useful throughout time.

A substantial number of [Organisation] datasets are released publicly either through data sharing arrangements or through dedicated applications or websites. These are supported by quality statements that support decisions about the usability of the data. Data available through DataVic is provided under Creative Commons licences.

[The Organisation] has in place an integration platform that supports use of data from multiple systems for analytics and reporting.

Some Groups/Divisions have developed or are developing their own capabilities to leverage their data for business intelligence and analytics. Other Groups/Divisions have found this challenging, resulting in inefficient integrations between systems.

The [central data repository] and Enterprise Data Catalogue aid access to / sharing information for business intelligence and analytics A limited number of key information assets have publicly available metadata documentation.

Data are shared securely in a number of ways, via [the Organisation] secure data exchange websites, or a dedicated Virtual Machines via the [secure virtual environment] for the analysis of de-identified linked and unlinked data.

Data are released to DataVic where appropriate.



[The Organisation] has a number of teams dedicated to responding to data requests from the public, researchers, other government [Organisations], and other parties.

An accreditation process for units that routinely share data has been instituted and requires units to undergo an assessment of their data management processes and training.

External data releases generally involve a data sharing agreement that requires the recipient to manage and dispose of data in accordance with legislation, the Information Privacy Principles and the VPDSS. Data integration and exchange starting to follow pattern-based architecture as outlined in target-state architecture.

[The Organisation] has a specific unit that has been accredited as an Integrating Authority to undertake complex integration and de-identification services for projects using Commonwealth dataset.

[...] [U]sers are currently using separate repositories and therefore different processes/practices.

The [central data repository] and Enterprise Data Catalogue aid access to / sharing information for business intelligence and analytics A limited number of key information assets have publicly available metadata documentation.

Data are shared securely in a number of ways, via [the Organisation] secure data exchange websites, or a dedicated Virtual Machines via the [secure virtual environment] for the analysis of de-identified linked and unlinked data.

Data are released to the public via [Organisation] websites and DataVic where appropriate.

[The Organisation] has a number of teams dedicated to responding to data requests from the public, researchers, other government [Organisations], and other parties.

An accreditation process for units that routinely share data has been instituted and requires units to undergo an assessment of their data management processes and training.

External data releases generally involve a data sharing agreement that requires the recipient to manage and dispose of data in accordance with legislation, the Information Privacy Principles and the VPDSS. Data integration and exchange starting to follow pattern-based architecture as outlined in target-state architecture.

Data collections use standard definitions, value domains and classifications wherever possible to support ease of reporting, comparison between data collections, years of data collections and comparison with national data.

[The Organisation] has a specific unit that has been accredited as an Integrating Authority to undertake complex integration and de-identification services for projects using Commonwealth dataset.

The [Business Unit] branch are 80% proactive, leveraging data and analytics to support informed decision making for government. Data exchanges occur in line with relevant legislation and standards are reviewed and retained with in [Organisational] guidelines. NextGen, (FES) are less advanced, with the remaining data capture areas in [the Organisation] in the aware category.

Business intelligence and analytics programs leverage information reuse.

Data analysts work with staff to ensure that data products can be used and reused over time. There are currently no documented processes that guide the use and reuse of information. No assessment has been conducted to date on the legal retention of data.

Data analysts work with staff to ensure that data products can be used and reused over time. There are currently no documented processes that guide the use and reuse of information. No assessment has been done to date on the legal retention of data.

[The Organisation's] Policies exist for data collection and its use both internally and externally.

Teams are able to use data to pull reports and understand digital environments on certain systems however there is not always visibility of all data from the broader organisation to assist in broader decision making.

Collected and processed data is utilised for reporting purposes and assists in strategizing, decision making and system planning of [Organisation]-related data as well as identifying general tasks to be undertaken and potential improvements.

Application Programming Interfaces (APIs) are used for the release of data in data exchange platforms with approved access using tokens.

Data collected in core decisions around budgeting, system planning and running reports on tasks such as Clean Ups, Transfers, Classifications, Ticketing and System (R365) Studies. All of this is the used to strategise, share live-data, protect data (thinking about security accesses and SAG setups etc).

Systems landscape is heavily reliant on disparate systems which results in duplicate handling of data as well as the potential for data quality concerns relating to source of truth. Internal Information Sharing Policy references the VPDSS and sets out contractual arrangements with third parties and other agencies, in order to document responsibilities and expectations around the security of information sharing and is reviewed annually. MOU Registers are accessible via the Intranet.

## 5 D4: Business Systems and Process

### 5.1 Business systems and processes: 4.1 Data architecture

#### From the questionnaire

Question:

- Has the organisation developed a data architecture model? To what degree does it link to other relevant models?

Examples of evidence:

- The organisation has developed a data architecture model which provides an overview and description of the organisation's data and their 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 data architecture aligns to other models such as the information technology and information architectures.

#### Supporting comments from participating organisations:

[The Organisation] is actively implementing VPDSS and IPP requirements, and has a cyber incident response plan defined. Privacy and security strategies are in place, and periodically assessed by assurance functions. Privacy and information security training are mandatory for all staff.

Whilst all our existing systems are documented, the systems are end of life and development has commenced on intended data architectures.

There is no overall [Organisation] data architecture model.

Some Groups/Divisions have their own models of varying sophistication or currency.

[The Organisation's] Architecture Review Board reviews proposed solutions for alignment with the Technology Strategy and the overall technology architecture and environment.

The Information Management projects employ a data architect/engineer.

Target state data architecture.

[The Organisation's] 'OurSystems' register captures and manages all Business Information Systems and their related business capabilities and supporting technologies which are regularly reviewed by the Architecture and Security teams.

[The Organisation's] digital roadmap outlines the current IT landscape, planned projects, and presents possible gaps and opportunities for where digital solutions can improve [the Organisation's] capability, capacity, and productivity.

[The Organisation] employs a standard process for initiating and conducting IT and digital projects that include defining business requirements, systems and processes and ensures alignment with [Organisation] strategies.

[The Organisation] does not currently have a data architecture model.

The Information Management projects employ a data architect/engineer.

Target state data architecture.

[The Organisation's] 'OurSystems' register captures and manages all Business Information Systems and their related business capabilities and supporting technologies which are regularly reviewed by the Architecture and Security teams.

Divisions of [the Organisation] have each developed their own digital roadmap (2024-25) outlining their current IT landscape, planned projects, and presents possible gaps and opportunities for where digital solutions can improve the division's capability, capacity, and productivity.

[The Organisation] employs a standard process for initiating and conducting IT and digital projects that include defining business requirements, systems and processes and ensures alignment with [Organisation] strategies.

Evidence and Insights are proactive in terms of data architecture in EDIE. AWS the EDIE platform has fully implemented data security in line with VPDS. Protective measures for staff are embedded in day-to-day processes. Retention and disposal have incorporated in the platform design. NextGen are less advanced having also designed retention and disposal into their data architecture, and security in line with VPDS. Other data collection repositories are much less advanced having an awareness of data architecture and working towards applying these to existing applications.

Present in new branches and groups but not consistent throughout [the Organisation].

[The Organisation] does not currently have a data architecture model.

[The Organisation] does not currently have an information architecture but the organisation is aware it needs to be done.

[The Organisation] has a data architecture model that is still in very early stages. This is most likely due to changes resulting from MoGs and staff movements.

A dedicated team is in place for data architecture to establish and implement measurements based on industry standards.

Raw format data can be ingested into or internal platform without transformation since tools implemented are not limited to any data format.

Security measures are in place in the technical architecture to reduce the risk of breaches.

Data systems are being standardised across the Victorian Government will stabilise information and allow for easier management of systems across larger entities but there will continue to be substantial challenges until this is achieved.

Gaps identified due to the number of disparate systems at various stages of their life cycle. Dedicated resource to map where the EDRMS Project and disclosure obligations fit within the IT and data architecture/ecosystem (in progress).

## 5.2 Business systems and processes: 4.2 Process improvement

### From the questionnaire

Question:

- How well have business processes been aligned with data management requirements?
- Has the organisation identified areas for improvement and eliminated duplicate processes?

Examples of evidence:

- Data management 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 data.
- Process issues impacting data management are directed to appropriate staff or working groups for action.
- Process owners are open to making changes to improve process and data management outcomes and develop/update process documentation accordingly.

### Supporting comments from participating organisations:

This kind of activity has been identified as a strategic goal, however, little has been done to date to really look at re-engineering business processes in this way. Incremental improvement is occurring as technology moves from legacy systems to modern platforms, the Digital Design and Innovation branch within [the business area] has a defined business engagement process to inform the design of new information and data systems, and their alignment with business requirements and efficient handling of information and data.

Data management practices are fairly mature and the responsibility of the Information Services team.

One responding team indicates they structure their planning processes around the emergence of stakeholder needs, and designs and builds workforce metrics infrastructure accordingly.

Process improvements to improve efficiencies and reduce duplication of data occur in Groups/Divisions on an as needs basis or as part of projects/programs.

Some Groups/Divisions are undertaking their own work to varying degrees based on whether there is sufficient capacity or prioritisation.

Processes have been introduced to streamline access and data sharing:

- The [central data repository] provide easier access to data across [the Organisation], by decoupling the operational systems, environments and integration from the sharing of the data from these systems.
- Units that release data on a regular basis can be 'accredited' to release data according to agreed delegations from the data custodian, removing the need to attain authorisation for each low-risk release.

Secure Data Exchange tool updated (SDE4).

Work is underway to establish [the Organisation's] processes; process improvement will follow.

Processes have been introduced to streamline access and data sharing:

- The [central data repository] provide easier access to data across [the Organisation], by decoupling the operational systems, environments and integration from the sharing of the data from these systems.
- Units that release data on a regular basis can be 'accredited' to release data according to agreed delegations from the data custodian, removing the need to attain authorisation for each low-risk release.
- New IT and data initiatives are assessed by the Project Initiative Assessment Group for alignment with IM Strategy before implementation.

Secure Data Exchange tool updated (SDE4).

Evidence and Insights are well progressed and proactive in terms of process improvement for data in the EDIE environment, the rest of [the Organisation] continues to lag behind. While the guardrails and engagement processes in TSDS are increasing awareness within the broader [Organisational] community about data sharing, reducing duplicate data capture etc, these processes are still in the early stages of adoption.

In progress as part of the Records365 rollout.

Data analysts work with specific teams on processes that incorporate data and data products into business activities; process issues identified and managed and resolved between the teams. No holistic assessment of where business processes might be engineered to take advantage of or align with data management requirements has yet been undertaken.

Data analysts work with specific teams on processes that incorporate data and data products into business activities; process issues identified and managed and resolved between the teams. No holistic assessment of where business processes might be engineered to take advantage of or align with data management requirements has yet been undertaken.

Staff are aware of [the Organisation's] data management practices.

[The Organisation] is dedicated to process improvement as seen through the promotion of Lean Six Sigma courses.

[The Organisation] has a dedicated Business Integration and Improvement group that are focused on process improvements.

Issues lay around providing people with access to tools and utilising capable talents properly to complete complex work that may lay beyond their core roles.

IM Assessments are embedded into our agile end-to-end process for ICT projects to ensure advice and recommendations align with statutory obligations and mandatory standards relating to retention, audits, accessibility and decommissioning. Established a Digital Transformation Committee (DTC) (internal tier 1 committee) including Sub-committees (SC) e.g. Data and IM SC and Cyber Security SC to enable subject matter experts to share opportunities and recommendations across the respective SCs and reporting to the DTC.

## 5.3 Business systems and processes: 4.3 Business systems and tools

From the questionnaire

Question:

- Are data management capabilities built into business systems and tools?

Examples of evidence:

- Data management specialists works together with Information Technology and risk management specialists as required to manage existing and/or implement new systems and tools.
- Data managed within the organisation's business systems and tools is effectively managed according to requirements from the Department of Government Services, Public Record Office Victoria, and Office of the Victorian Information Commissioner.
- The organisation encourages and adopts improvements to system and tool data management capabilities.
- Systems and tools are effectively managed over their life, from acquisition to decommissioning, to ensure their integrity, reliability, and performance.

### Supporting comments from participating organisations:

Although the process is still undergoing incremental refinement, procedures are in place to ensure that information and data managed within [the Organisation's] business systems and tools is managed according to policy and regulatory requirements.

One responding team indicates they structure their planning processes around the emergence of stakeholder needs, and designs and builds workforce metrics infrastructure accordingly.

The responding external statutory authority indicates that data management specialists in their Information Services team manage all data related activities.

[The Organisation's] Architecture Review Board ensures that new applications and systems are conforming to the relevant standards.

[The Organisation] has in place an integration platform that supports use of data from multiple systems for analytics and reporting.

There have been local investments which incorporate data management specialists working together with information technology and risk management specialists as required to manage existing and/or implement new systems and tools.

In other cases, Groups/Divisions are rationalising the number of tools in place, while in other cases systems are being built without consulting data specialists.

[central data repository] implemented.

Purview Data Catalogue implemented.

Secure Data Exchange tool updated (SDE4).

Access to sensitive, linked datasets enabled via the [secure virtual environment].

Effective Data management is occurring in specific teams and applications, however there is no holistic program to assess and improve data management overall.

[central data repository] implemented.

Purview Data Catalogue implemented.

Secure Data Exchange tool updated (SDE4).

Access to sensitive, linked datasets enabled via the [secure virtual environment].

Enable [business function] service staff to access data in the VAHI Information Management Environment (VIME).

See answers above [ie – supporting comments for previous questions].

[The Organisation] promotes and embraces enhancements to the data management capabilities of its systems and tools.

Information Security liaises with teams to assess incoming systems to ensure they meet data protection requirements. [The Organisation] has specific data management tools and systems to manage and present data, such as dashboards. No assessment has been undertaken on these systems to determine compliance with DGS (WOVG Information Management Framework), PROV and OVIC requirements.

Information Security liaises with teams to assess incoming systems to ensure they meet data protection requirements. [The Organisation] has specific data management rolls and systems to manage and present data, such as dashboards. No assessment has been undertaken on these systems to determine compliance with PROV and OVIC requirements.

Data is managed through business systems, tools and policies with [the Organisation] upgrading systems to improve the handling and disposal of data.

Metadata is contained and protected according to Government requirements, such as PROV and OVIC.

The majority of the stored information is managed, processed and released through a cloud-based environment. This is managed internally with a dedicated team monitoring activities daily to ensure the services are running correctly with mitigations in place if a process fails.

The management of data includes agreed intervals of processing, release management of new and updated information and notifications to relevant parties with resolution timeframes when issues arise.

IM Assessments are embedded into our agile end-to-end process for ICT projects to ensure advice and recommendations align with statutory obligations and mandatory standards relating to retention, audits, accessibility and decommissioning. Established a Digital Transformation Committee (DTC) (internal tier 1 committee) including Sub-committees (SC) e.g. Data and IM SC and Cyber Security SC to enable subject matter experts to share opportunities and recommendations across the respective SCs and reporting to the DTC.

## 5.4 Business systems and processes: 4.4 Privacy and security

### From the questionnaire

Question:

- What is the status of data privacy and security in the organisation?
- Do staff have the knowledge and support to protect data and ensure their confidentiality, integrity, and availability?
- Is the organisation able to respond to data privacy and security incidents?

Examples of evidence:

- The organisation is actively implementing requirements outlined in the Victorian Protective Data Security Standards, the Information Privacy Principles, and the Victorian Government Cyber Incident Management Plan.
- The organisation has data privacy and security strategies in place and an assurance program in place to manage privacy and security risks. 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 data 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 Data Security Incident Notification Scheme.

### Supporting comments from participating organisations:

[The Organisation] is actively implementing VPDSS and IPP requirements, and has a cyber incident response plan defined. Privacy and security strategies are in place, and periodically assessed by assurance functions. Privacy and information security training are mandatory for all staff.

One responding team indicates in every data and analysis provision, the team conducts a rigorous assessment of confidentiality risk and discusses with executives to seek decision on tradeoffs between responsiveness and protection of staff confidentiality and data security.

Some elements of data management rely on [the Organisation's] [business area's] processes and at this base level there may be vulnerabilities given there is a lack of transparency in the services provided to external agencies by [the Organisation].

[The Organisation] has an ongoing cyber security and assurance program, a cyber security strategy and information privacy program to manage data privacy and security risks.

[The Organisation] is actively implementing its Protective Data Security Plan in line with the Victorian Protective Data Security Standards and Information Privacy Principles.

Privacy impact assessments and security assessments are carried out for new application and system developments.

All staff must undertake [the Organisation's] privacy eLearning.

[The Organisation] has a Cyber Incident Response procedure. Incidents are reported in line with the Information Security Incident Notification Scheme.

[The Organisation] has a Security and Privacy Committee with representation from all Groups to review and advise on security and privacy related matters.

[The Organisation] has a security help desk for staff to report issues and raise service requests.

[The Organisation] runs regular programs to measure its cyber security maturity (eg phishing campaigns) and inform improvement initiatives.

[The Organisation] produces a regular security performance report to measure progress and inform improvement initiatives.

A review of the Information Security Incident Management process has been completed and findings from that review will inform uplift to incident reporting and management.

Protective Markings have been rolled out to comply with Victorian Protective Data Security Standards (VPDSS).

Security by design is integrated into the Agile Project Operating Model (APOM) to ensure that security is front of mind during the project lifecycle.

[The Organisation] employs privacy by design, aiming for privacy to be 'built in' to any activities or initiatives that may have privacy implications. Facilitated by staff doing Privacy Impact Assessments (PIA) as part of a project, for example the ICT Project Complexity Assessment tool – a key document required at [the Organisation's] Project Initiative Assessment Group (PIAG), indicates whether a Threshold Privacy Assessment or PIA is required dependant on inputs received from the user as to whether the project is dealing with client or clinical information. [The Organisation's] PIAs are designed to be consistent with OVIC requirements, and include formal, written assessments of privacy, information security and (as relevant) record-keeping obligations in relation to projects that involve the collection, use or disclosure of personal information. Completed PIAs identify privacy 'to do' items for project proponents to implement.

The Privacy and Legal Compliance Team advise on privacy matters. The Privacy websites include resources and training material for [Organisational] staff. The Privacy and Legal Compliance Team has also championed the use of a PIA register by Division to encourage more regular references to PIAs post implementation including consideration of whether a fresh review is required due to changes in scope; and knowledge sharing where appropriate.

All staff complete the Privacy Awareness and Cyber Security eLearning modules.

[The Organisation] is standardising operational management of privacy incidents via a consolidated statewide approach.

[The Organisation] has established a Privacy and FOI Office which is operational.

A range of foundational policies for information and cybersecurity are underway.

[central data repository] has managed and governed access to data.

Access to sensitive, linked datasets enabled via the [secure virtual environment].

...[S]ervice staff are able to access data using the VAHI Information Management Environment (VIME).

A secure data exchange is used for transferring data to external organisations.

Staff are aware of information security and privacy requirements, policy, and legislation.

Information Security Management Framework (ISMF) is currently under review. Feedback management system (FMS) privacy module: enterprise system for end-to-end privacy incident management.

New system procurement requires prospective IT vendors to complete a set of security questions, that are based on the newly implemented Third Party Standards, as part of the solution based on the information security classification and business requirements.

[The Organisation] has developed a set of eighteen Information Security Standards that set out specific security controls or 'safeguards' for business units, [Organisational] staff, contractors or third parties to adhere to and implement.

Security assessments are performed based on the Australian Signals Directorate ISM framework, [the Organisation's] new information security standards and existing WoVG Security Policies and Standards (Information Security Classification, Privacy Impact Assessment, Third-party gap assessment, System Security Plan, Penetration Test and Risk assessment and mitigation).

External system penetration tests carried out bi-monthly, and regular (yearly) security tests are conducted on critical systems and applications.

The Cyber Security Team collaborates and provides awareness on security emerging issues as they arise via Viva Engage and the Cyber Security SharePoint site, including cyber security alerts and resources to promote working from home securely.

A review of the Information Security Incident Management process has been completed and findings from that review will inform uplift to incident reporting and management.

Protective Markings have been rolled out to comply with Victorian Protective Data Security Standards (VPDSS).

Security by design is integrated into the Agile Project Operating Model (APOM) to ensure that security is front of mind during the project lifecycle.

[The Organisation] employs privacy by design, aiming for privacy to be 'built in' to any activities or initiatives that may have privacy implications. Facilitated by staff doing Privacy Impact Assessments (PIA) as part of a project, for example the ICT Project Complexity Assessment tool – a key document required at [the Organisation's] Project Initiative Assessment Group (PIAG), indicates whether a Threshold Privacy Assessment or PIA is required dependant on inputs received from the user as to whether the project is dealing with client or clinical information. [The Organisation's] PIAs are designed to be consistent with OVIC requirements, and include formal, written assessments of privacy, information security and (as relevant) record-keeping obligations in relation to projects that involve the collection, use or disclosure of personal information. Completed PIAs identify privacy 'to do' items for project proponents to implement.

The Privacy and Legal Compliance Team advise on privacy matters. The Privacy websites include resources and training material for [Organisational] staff. The Privacy and Legal Compliance Team has also championed the use of a PIA register by Division to encourage more regular references to PIAs post implementation including consideration of whether a fresh review is required due to changes in scope; and knowledge sharing where appropriate.

All staff complete the Privacy Awareness and Cyber Security eLearning modules.

[The Organisation] is standardising operational management of privacy incidents via a consolidated statewide approach.

While Evidence and Insights have in their EDIE AWS environment fully implemented data security in line with VPDS. Protective measures for staff are embedded in day-to-day processes and PIAs are being reviewed. NextGen have completed PIA's and IARs'. In terms of smaller data repositories, PIA's and IARs exist for some not all, however this is improving as new applications/platforms undertake our guardrail processes around information management prior to deployment. This process has recently been extended to include application upgrades.

[The Organisation] has submitted a PDSP and attestation since its inception as well as former [Organisations]. OVIC is notified of breaches. PIAs, security checklists, and risk assessments is embedded in procurement processes. There are dedicated teams at a corporate level for support.

Compliance to the Data standards not well developed. [The Organisation] has actively engaged a program of work to implement the requirements outlined in the Victoria Protective Data Security Standards.

[The Organisation] has actively engaged a program of work to implement the requirements outlined in the Victoria Protective Data Security Standards including:

- regular attestation
- security strategies
- assurance program
- Has conducted PIAs
- ITS incident response plan.

[The Organisation] has established data privacy and security strategies in place to manage privacy and security risks.

[The Organisation's] learning management system contains mandatory e- Learning modules related to privacy and data protection that are undertaken by staff on commencement and then on a biennially basis.

All staff have access to Data Privacy information available on [the Organisation's] intranet with additional ad-hoc information sessions and articles provided for staff.

The Cyber security and Privacy branch coordinate well on Information Security Value Assessments (ISVA) and Privacy Impact Assessments (PIA) and rigorous privacy assessments are undertaken by a dedicated team with determinations on Business Impact Levels (BIL).

Data and metadata are adequately secured through access controls in online databases.

Breach responses are generally timely and follow accepted practice, including notifications to OVIC.

Cyber Security Strategy 2022-2025 approved by senior management. We are currently into year two of implementation and have had a significant uplift in security tools, risk management and education. Dedicated information and cyber security training resources appointed and refreshed course content.

Protective Security Portfolio Holders across the organisation supporting information and security and cyber security practices. Aligned with the VPDSS annual attestation provided to OVIC (2024 PDSP and attestation rating = core). Dedicated security risk assessment team and security risk management function. Security Incident Management Plan and playbooks in-place.

Implementation of the IBM security operations centre (best of breed) for security monitoring. Dedicated Security Incident Registry which continues to capture all security and privacy incidents. Privacy Policy review (in-progress), Cyber Security Sub-committee established, successful prosecutions against offences under relevant legislation.

## 6 D5: Data Integrity (Optional)

### 6.1 Data integrity: 5.1 Sharing, access, integration and interoperability

#### From the questionnaire

Question:

- Are data sharing, integration and interoperability capabilities built into business systems, processes, and tools?

Examples of evidence:

- The organisation is actively implementing the responsibility to share as outlined in the VPS Data Sharing Policy and uses the VPS Data Sharing Heads of Agreement when sharing data with another party. The organisation complies with the Information Privacy Principles, the Victorian Protective Data Security Standards, the Data Exchange Framework and Victorian Government Data Directory Metadata Standards. There is a clearly defined governance structure for overseeing data sharing activities, including roles and responsibilities. The organisation has documented and communicated policies and processes outlining how data sharing is managed, including legal and ethical considerations.
- The organisation maintains a data sharing register and consistent practices for data access and provenance. The organisation ensures the privacy, security, and integrity of shared data by using risk assessments, encryption, access controls and secure transfer mechanisms, where appropriate. The organisation keeps comprehensive documentation outlining data sources, methodologies, and any transformations applied. The organisation regularly engages with data users for feedback and showcases tangible benefits or innovations resulting from the use of their data. This includes quantifying evidence of positive outcomes or improvements from data sharing collaborations. Established processes are in place to: make, review, and respond to a data sharing request. Employees receive ongoing training to share data safely. The organisation lists its shareable data in the Victorian Data Directory.

#### Supporting comments from participating organisations:

[The Organisation] has written the responsibility to share into an approved [Organisational] information sharing standard. Regulatory requirements are incorporated into data sharing and integration assessment activities. The data governance operating model sets out the governance structure covering these activities, with roles and responsibilities defined. More could be done to improve adherence to these defined requirements.

One other respondent has indicated their team regularly develops data infrastructure for other teams and external organisations (e.g., policy and program evaluators).

The responding external agency is a signatory (separate to [the Organisation]) of the VPS Data Sharing Heads of Agreement and has utilised the agreement to work with external government [Organisations]. We also have a formal data request process, and this requires sign-off by the



delegate or Deputy CEO, [Business Unit] as the data owner. We make data available to assist other co-regulators and also work effectively with the commonwealth.

[The Organisation] has in place an integration platform that supports use of data from multiple systems.

The IM team provides guidance and supports [the Organisation] to share data in accordance with the VPS data sharing framework.

Data custodians are encouraged to register suitable data assets on DataVic.

The Data access and release policy and guide describe the requirements for data sharing. The process includes legal considerations, assessment of risk, the means by which information can be shared, conditions of use, information governance arrangements, record keeping obligations.

[The Organisation] encourages data sharing between Victorian government agencies and uses the VPS Data Sharing Heads of Agreement when sharing data with another party.

A data release accreditation process enables teams that release data on a regular basis to become accredited to release certain data without requiring authorisation from the custodian for each release.

[The Organisation] maintains an information sharing agreement register for all information sharing agreements. Compliance with this is quite limited at the present time.

This is currently unknown by the Information and Security Branch.

The IM team provides guidance and supports [the Organisation] to share data in accordance with the VPS data sharing framework.

Data custodians are encouraged to register suitable data assets on DataVic.

The Data access and release policy and guide describe the requirements for data sharing. The process includes legal considerations, assessment of risk, the means by which information can be shared, conditions of use, information governance arrangements, record keeping obligations.

[The Organisation] encourages data sharing between Victorian government agencies and uses the VPS Data Sharing Heads of Agreement when sharing data with another party.

A data release accreditation process enables teams that release data on a regular basis to become accredited to release certain data without requiring authorisation from the custodian for each release.

[The Organisation] maintains an information sharing agreement register for all information sharing agreements. Compliance with this is quite limited at the present time.

Standard datasets are made available annually to public [function] services that contribute to [sector] data sets.

Whilst a couple of areas of [the Organisation] are actively implementing VPS Data sharing policy and uses the VPS Heads of agreement for sharing data with another party from their repository, other areas within [the Organisation] remain at the opposite end of the spectrum, not fully understanding their obligations and responsibilities, (data management is an emerging discipline).

As previously mentioned in 4.1 we have a guardrail process that applications go through, and one of the key criteria is interoperability and the use of common APIs. Our Evidence and Insights area is currently reviewing its policies and processes around data sharing management including legal and ethical considerations for the EDIE data lake.

Data sharing is still not fully mature across [the Organisation].

## 6.2 Data integrity: 5.2 Open data

### From the questionnaire

Question:

- Is the organisation's data release timely and accurate?

Examples of evidence:

- The organisation is actively implementing requirements outlined in the DataVic Access Policy and the Whole of Victorian Government Intellectual Property Policy.
- The organisation has developed an internal open data policy and process.
- The organisation regularly engages with the community for feedback and showcasing tangible benefits or innovations resulting from the use of their open data.
- The organisation consistently releases relevant, up-to-date data in accessible formats.
- The organisation integrates the publication of open data into the group's work practices.
- Staff have the knowledge and support to open data safely.

### Supporting comments from participating organisations:

[The Organisation] has defined an Information and Data Release standard aligned to WoVG policies, and has a mature open data process - however more could be done to identify and publish datasets more relevant to researchers and the public.

One respondent indicates their team maintains a strong focus on responsiveness in constructing analyses to respond to a large volume of incoming ad-hoc requests and regular reporting requirements.

The responding external statutory agency indicates they believe in having as much open data as possible including the publicly available state register however they currently do not publish to DataVic.

A substantial number of [Organisation] datasets are released publicly either through data sharing arrangements or through dedicated applications or websites.

In other cases, data is provided when required for specific timelines, but also in an ad hoc way and irregularly.

Data custodians are encouraged to register suitable data assets on DataVic.

This is currently unknown by the Information and Security Branch.

Specific ... data are made publicly available on a regular basis through the Victorian ... website.

Data collected through the Victorian ... Survey are made available to the public on [the Organisation's] website.

Data custodians are encouraged to register suitable data assets on DataVic.

Our Evidence and Insight CSA output datasets are in the Victorian Data Directory.

No practical evidence. [The Organisation] now has access to DataVic.

ET does complete the ISVA process to determine if data can be released in public domain.

Targets for data release, community engagements for projects, formal FOI process.

The organisation is very supportive of the Open Data platform ([www.data.vic.gov.au](http://www.data.vic.gov.au)) which holds 177 datasets with Metadata and posts regular updates to them.

A new open data platform (by [the Organisation]) is currently under development to proactively release the datasets into open data using cloud technologies to meet the growing demand of the open data sets.

Some of these datasets are highly sought by the public....

Currently the organisation is transparent.

Supported through a number of legislation, schemes, MOUs, partnerships to provide accessible data in formats that support government decision making, circumstances where it is required to provide available services FOI, Corporate Services and Community Services.

## 6.3 Data integrity: 5.3 Data and AI ethics

### From the questionnaire

Question:

- What is the status of data ethics in the organisation?
- Do staff have the knowledge and support to ensure the ethical use of data?
- Is the organisation able to respond to incidents involving the unethical use of data?

Examples of evidence:

- The organisation has well defined ethical guidelines for data and artificial intelligence (AI) use.
- Employees receive ongoing training on data and AI ethics to ensure awareness and understanding of ethical consideration.
- The organisation promotes transparency by openly communicating its AI processes, decision-making criteria and potential biases.
- Strategies are implemented to identify and mitigate biases in algorithms, ensuring fairness in AI applications.
- Stakeholders, including end-users, are actively involved in the development and deployment of AI systems to incorporate diverse perspectives.

- The organisation conducts regular audits and assessments of AI systems to identify and address ethical concerns proactively.
- The organisation has appropriate plans in place which are reviewed and maintained (such as a Data Ethics Incident Response Plan). The organisation has clear procedures and points of contact to seek out guidance regarding data and AI ethics.
- The organisation only applies AI tools to data that:
  - would otherwise be accessible to the user
  - is appropriately labelled/classified.

### **Supporting comments from participating organisations:**

An AI strategy has been commissioned and is under development. Currently data ethics is managed in line with the ordinary decision making process of the organisation - more could be done to clearly define and communicate best practices in this area.

There is a general awareness and some understanding, but it is inconsistent across the organisation.

Approaches to date have been conservative, in some cases due to concerns about data integrity and lack of confidence in the accuracy of the classification/sensitivity attribution on data.

[The Organisation] has published instructions on the intranet about preventing a data breach while using generative AI tools at work.

[The Organisational] Artificial Intelligence (AI) Usage Policy has been developed to support a structured approach to incorporating Artificial Intelligence (AI) technologies into [the Organisation's] daily operations. Pockets of [the Organisation] are aware of and manage the implications of ethics and the use of AI, but work is required to uplift maturity across the board.

A VPS AI Assurance Framework has been developed by the DGS Cyber Security, Data and Digital Resilience Division to operationalise the National Framework for the Assurance of AI in Government for the VPS. The Framework:

- is designed to support the safe and responsible delivery of AI in the VPS, by promoting transparency and accountability, and a common approach to identifying, evaluating, communicating, and managing the ethics and risks associated with AI use cases
- is comprised of a self-assessment tool and guidance material, and adopts Australia's AI Ethics Principles, consistent with the National Framework.

[The Organisation] has developed General Artificial Intelligence Guidance that complies with the WoVG policy.

The AI taskforce oversees the use of AI in the ... sector.

M365 Copilot feasibility assessment carried out, resulting in intention to rollout Copilot through [the Organisation's] service catalogue in 2025.

Our Evidence and Insights area has policies and processes around the legal and ethical considerations for use and sharing of its data, this is currently being reviewed, and [the Organisation] currently has a draft AI policy. Whilst the AI policy will have global coverage, other data management and use policies currently only cover data stored in EDIE.



There is a use of AI policy however data quality and governance is not mature.

Interim Gen AI policy.

Initial Gen AI training and awareness sessions.

Co-pilot program.

Investigation of AI tools and capability.

Greater communication and awareness is still needed, field is rapidly progressing.

Done a POC to explore the options of AI to understand the impact on [Organisational] data.

Part of the Data & Digital 2024/2025 goals (-) Scoring points for ethical questions such as race, religion. etc

AI Ethics Framework aligns with enabling principles e.g. Human Rights, Community Benefit, Fairness, Privacy and Security, Transparency, Accountability, Human oversight and Skills and Knowledge. Also aligns with internal policies e.g. IM and Information Security, Appropriate Use of Information, Use, Handling and Storage and Information Sharing. Organisation has communicated their AI position to further support consistency in the understanding of AI enterprise wide. Established strong governance through senior leadership, conversation and activities via DTC and Sub-committees.

## 6.4 Data integrity: 5.4 Data quality

### From the questionnaire

Question:

- How well does the organisation identify, address, and monitor data quality issues?
- Is the organisations data of high quality?

Examples of evidence:

- The organisation has procedures or systems in place to ensure the integrity, usability and maintenance of data assets.
- The organisation is alerted when data quality degrades and can adequately and quickly address, respond to or remediate any issues.
- The organisation captures and maintains metadata for key data assets (structured, semi-structured, and structured).
- The organisation has developed an internal data quality strategy or defined goals for data quality.
- The data produced by your organisation is assessed against data quality attributes, such as the dimensions listed in the Victorian Government Data Quality Guideline or the Data Quality chapter of the DAMA International Data Management Book of Knowledge. For example, the organisation's data is assessed for its completeness, timeliness accuracy, consistency, uniqueness and validity.

## Supporting comments from participating organisations:

[The Organisation] has defined a data quality management framework, however this remains to be widely rolled out and communicated to staff. Beyond this, there are pockets of good data quality management, and pockets where data quality management is immature.

As any database has limitations, the team balances producing informative workforce analytics, explaining limitations to stakeholders, limiting respondent burden when considering database improvements, and developing proxy metrics where full data is not collected.

The Information Services team of the responding external agency currently has an active campaign to increase data quality through regular monitoring and working with business units to remediate any identified issues.

There are activities in place to identify, address and monitor data quality, but they aren't consistent across [the Organisation].

In some Groups/Divisions data quality is dependent on programs/initiatives but is not continuously managed. Others have developed their own internal data quality strategy. In other cases, a lack of auditing/quality control measures have resulted in inaccurate data and/or data lacking integrity being held in information systems.

The Data quality policy describes the minimum requirements for managing [the Organisation's] information assets.

The Data quality guide describes the requirements for managing data quality of our information assets and how to assess the quality of an asset using the data quality assessment tool.

Dataset administrators are responsible for assessing the quality of their information assets using the data quality assessment tool. Custodians are responsible for ensuring this occurs.

Data quality considerations form a part of the data collection design and development stages for majority of [Organisation] information assets.

The Information Management team runs a program to educate custodians and administrators about responsibilities under the Data Quality Policy, and to assist in the completion of mandatory artefacts.

[The Organisation] is aware that its information assets and data assets need to be captured and classified. Currently both are captured in the Information Asset Register, but are not distinguished from each other.

The Data quality policy describes the minimum requirements for managing [the Organisation's] information assets.

The Data quality guide describes the requirements for managing data quality of our information assets and how to assess the quality of an asset using the data quality assessment tool.

Dataset administrators are responsible for assessing the quality of their information assets using the data quality assessment tool.

Data quality statements are available for some information assets (mainly the [business function] data collections).

Data quality considerations form a part of the data collection design and development stages for majority of [Organisation] information assets.

Data integrity audits are carried out for some [business function] data collections.

The Information Management team runs a program to educate custodians and administrators about responsibilities under the Data Quality Policy, and to assist in the completion of mandatory artefacts.

Our EDIE environment has automated processes in place to ensure data quality, the same cannot be said or guaranteed for other data repositories within [the Organisation].

No practical evidence.

This has such great variance across [the Organisation] depending on the type of data.

Data Quality testing framework that is currently implemented in the data platform (used with the Databricks) which impacts data sets stored and processed in the [Organisation] Data Platform.

Data Governance IDQ (Informatica Data Quality) application is discontinued due to inadequate usage.

Users are conducted testing on the processed data to ensure that released ... reporting tools are producing accurate results to our consumers.

Systems, policies and processes in place across core systems to enable operationalising of critical service delivery and functions. Internal framework is supported through multiple legislation, schemes and established MOUs.

## 6.5 Data integrity: 5.5 Data availability

### From the questionnaire:

Question:

- Is data available to meet the needs of the business and its users?

Examples of evidence:

- The organisation employs redundant systems and backups to ensure continuous data availability in the event of hardware failures or other disruptions.
- Continuous monitoring tools are in place to promptly identify and address issues that could impact data availability, allowing for proactive responses.
- Remediation processes are in place to address availability issues, with a clear and documented escalation path as part of the process, and remediation actions required prioritised and addressed.
- Routine and comprehensive data backups are conducted, allowing for quick restoration in case of data loss or corruption.
- Robust security measures are implemented to prevent unauthorised access or cyber threats that could compromise data availability.

- Effective user support mechanisms and communication channels are in place to promptly address user concerns and inform them of any disruptions or maintenance activities affecting data availability.

#### **Supporting comments from participating organisations:**

The [board] governs the implementation of information technology changes which produce expectations or risks of downtime. Availability of [the Organisation's] cloud applications and services are protected by redundancy arrangements through Azure.

One respondent indicates their team has a heavy workload in providing large volumes of ad-hoc data and analysis requests and regular workforce reporting.

Whilst highly dependent on [the Organisation] for infrastructure support, monitoring occurs both by [the Organisation] and the responding external statutory agency to ensure availability.

There are activities in place to ensure data is available to meet the needs of the business and its users, but there isn't a consistent approach across [the Organisation].

In some Groups/Divisions, continuous monitoring tools are in place to identify and address issues that could impact data availability, allowing for proactive responses. In other cases, limited data is available as data is siloed and not integrated, or users do not have the necessary permissions or tools to access the data they need. There are no clear policies or procedures for managing data.

The organisation employs redundant systems and backups to ensure continuous data availability in the event of hardware failures or other disruptions.

Continuous monitoring tools are in place to promptly identify and address issues that could impact data availability, allowing for proactive responses.

Remediation processes are in place to address availability issues, with a clear and documented escalation path as part of the process, and remediation actions required prioritised and addressed.

Routine and comprehensive data backups are conducted, allowing for quick restoration in case of data loss or corruption.

Robust security measures are implemented to prevent unauthorised access or cyber threats that could compromise data availability.

Effective user support mechanisms and communication channels are in place to promptly address user concerns and inform them of any disruptions or maintenance activities affecting data availability.

The CIOs of [the Organisations] jointly oversee the Disaster Recovery (DR) capabilities of their [Organisations'] IT systems through various governance forums.

All corporate data assets have availability controls in place and disaster recovery is tested regularly. The Information and Security Branch needs to engage with the line of business application owners to confirm similar controls are in place and effective.

The organisation employs redundant systems and backups to ensure continuous data availability in the event of hardware failures or other disruptions.

Continuous monitoring tools are in place to promptly identify and address issues that could impact data availability, allowing for proactive responses.

Remediation processes are in place to address availability issues, with a clear and documented escalation path as part of the process, and remediation actions required prioritised and addressed.

Routine and comprehensive data backups are conducted, allowing for quick restoration in case of data loss or corruption.

Robust security measures are implemented to prevent unauthorised access or cyber threats that could compromise data availability.

Effective user support mechanisms and communication channels are in place to promptly address user concerns and inform them of any disruptions or maintenance activities affecting data availability.

The CIOs of [the Organisations] jointly oversee the Disaster Recovery (DR) capabilities of their [Organisations'] IT systems through various governance forums.

Evidence and Insights have achieved fully automated data storage, reporting, and management through SharePoint, Power Automate workflows and Power BI. Security measures such as those listed are covered off via the EDIE project and AWS working environment. NextGen has ASAE 3402 audit report, full back up cycle, daily system checks and monthly operational reporting. Other smaller data collections are unknown.

All corporate critical systems have disaster recovery and backup plans.

System Back Up and Recovery Standard.

Disaster Recovery Plan.

When a processing job fails in the internal system, they are re-run after the remediations, and testing is completed.

Responding to customer requesting seeking clarification if datasets are not available in our platforms or Open Data.

Monitoring of available datasets to proactively ensure no errors are found.

Legacy platforms with many datasets ... are available via modern platform through [Organisation] Data Platform.

Established daily back-up reporting for ongoing monitoring with annual back-up restore validation completed across all class 1 applications.

Regular disaster recovery planning and testing in place to validate fail-over between data centres to protect against hardware failure.

## 6.6 Data integrity: 5.6 Indigenous Data Sovereignty

### From the questionnaire

Question:

- Does the organisation have a robust data sovereignty program that safeguards data in accordance with legal and regulatory requirements?
- Do staff have the knowledge and support to implement data sovereignty initiatives in the organisation, where possible?

Examples of evidence:

- The organisation has an Indigenous Data Sovereignty strategy and implementation plan or program of work in place, that has been communicated to staff.
- The organisation's data governance framework includes roles and responsibilities for managing Indigenous Data Sovereignty, ensuring accountability. Indigenous Data Sovereignty is considered in the organisation's data privacy, security and ethics frameworks and processes.
- The organisation has mechanisms in place to enable transparent communication with stakeholders about Indigenous Data Sovereignty measures in place, fostering trust and understanding.
- There are training initiatives in place to educate employees and stakeholders about the importance of Indigenous Data Sovereignty and their role in maintaining compliance.
- Prior to implementing new data processes, the organisation conducts thorough assessments to understand and mitigate any potential impacts on Indigenous Data Sovereignty.

### Supporting comments from participating organisations:

Although Indigenous Data Sovereignty has been identified as a future item to be addressed, limited concrete steps have been taken toward its implementation.

One respondent indicates not applicable to our team, beyond the handling of ATSI status in line with the broader, overall approach to protecting staff confidentiality.

The responding external agency takes a position that information retention is critical particularly in relation to indigenous data sovereignty however as the holders or sometimes incomplete information from defunct organisations and government [Organisations] identifying relevant data can be difficult however the VRQA takes a conservative retention approach which mitigates issues to a degree whilst a more formal approach can be defined.

[The Organisation] has developed a pathway to an Indigenous Data Sovereignty Policy and an accompanying program of work to implement the pathway. There is some awareness of indigenous data sovereignty, but it is limited to date.

[The Indigenous] Division leads the work to develop ADS direction and principles.

[The Organisation] has developed a Victorian Government First Peoples Data Sovereignty draft workplan, alongside a First Peoples policy workplan that identifies WOVG and [Organisation] wide actions to implement Indigenous Data Sovereignty (IDS) principles and practices. These workplans

support key government policy activities for Treaty preparedness, Truth-telling and Self-determination.

There is also a general understanding of IDS in [the Organisation] with a number of intersecting work programs that support this work across government.

[The Indigenous] division leads the work to develop ADS direction and principles, supported by the IM team for implementation guidance.

Evidence and Insights have mechanisms in place within the EDIE data lake to enable transparent communication with stakeholders about Indigenous Data Sovereignty measures in place fostering trust and understanding making them proactive. We have no evidence about data holdings outside of Evidence and Insights.

[The Indigenous Business Unit] has drafted a Data Sovereignty strategy and is pending for approval.

The wider organisation is unaware.

Indigenous Data Sovereignty (IDS) is a commitment through the Victorian Aboriginal Affairs Framework 2018-2023 and the Victorian Government Self-Determination and Reform Framework and is one of the recommendations to come out of the Yoorrook Justice Commission truth-telling process - [the Organisation is] in the beginning phase of developing an IDS strategy.

Commitment by the head of the agency and senior management on the delivery of a statement of commitment actions by the end of 2025 including to explore the viability of operationalising Indigenous Data Sovereignty across [the Organisation] e.g. the identification and capture of Indigenous Data Sovereignty information/records (in-progress). Currently drafting a Data Governance Framework for broader internal engagement and exploring opportunities to improve existing records management practices based on the learnings from the current Yoorrook Justice Commission Inquiry.

