Australian Government
Department of Finance

Chief Data Officer Information Pack

Version	Issue Date
Chief Data Officer Information Pack v1.0	March 2024

Contents

Introduction

Australian Government Chief Data Officers (CDOs) are accountable for their organisation's enterprise-wide governance and use of data as an asset, as well as building agency data capabilities. This accountability involves not only the formal responsibilities but will include meeting the Government's expectations for APS agency data management and use.

APS CDOs also operate within a broad and complex Commonwealth data system, comprising many cross-cutting data initiatives, policies, frameworks, and data assets led by a multitude of data stakeholders.

This Information Pack has been developed to help CDOs understand their accountabilities and how their role fits into the broader Commonwealth data system.

We encourage CDOs to use the information in this pack to guide and support decision making that will suit the requirements for their individual agencies. The pack should not be read as an exhaustive list or a directive of how CDOs should design or fulfill their roles for their agencies.

This Information Pack will help CDOs to:

- understand their accountabilities and the Government's expectations (**Section 1**);
- navigate the Commonwealth data system (**Section 2**);
- build awareness of APS data governance groups and other communities (**Section 3**);
- contact relevant stakeholders (**Section 4**); and
- access additional resources (**Section 5**).

The Department of Finance (Finance) welcomes feedback on the Information Pack and will update it regularly in collaboration with the Data Champions Executive/Network.

For further information on this pack, please visit the Data Policy webpage or contact Finance's Data Policy team (DataPolicy2@finance.gov.au).

1. Chief Data Officer responsibilities

> "Senior leaders of the APS must be held accountable for the quality of their data assets. … Building a data-driven culture will require overcoming the culture of risk aversion and legislative barriers that prevail in the APS."
>
> – Independent Review of the Australian Public Service (2019).

Finance has developed the SES Accountabilities for Data product, which sets out guiding principles regarding the roles of SES and equivalent officers in improving data accountabilities. This document should be read alongside the Foundational Four, released by the Office of the National Data Commissioner (ONDC) in 2020, which sets out four pillars for good data governance. Further detail on the SES Accountabilities for Data product and the Foundational Four is provided below.

While each APS agency has broad autonomy for setting the roles and responsibilities for its CDO, the SES Accountabilities for Data product affirms the following **actions for which all Australian Government CDOs are accountable and cannot delegate responsibility**:

- fostering the creation of a data-driven culture that harnesses the value of enterprise data assets to inform decision-making;
- building and maintaining positive relationships with the agency's other senior leaders, and promote opportunities for data to improve business outcomes;
- working with other senior leaders to ensure data security and protection, including safe storage and confidentiality; and
- building capability of other CDOs (e.g. by participating in cross-agency recruitment panels, mentoring new CDOs, sharing knowledge).

CDOs should work closely with other officials in their agencies with cross-cutting responsibilities such as the Chief Information/Digital Officer, Chief Risk/Governance Officer, Chief Security Officer and/or Chief Data Analytics Officer. The specific distribution of responsibilities among these roles is at the discretion of individual agencies and will depend on factors including their size and operational responsibilities. Refer to the SES Accountabilities for Data report for more guidance on other data-related roles and their interaction with CDOs.

APS CDOs and other relevant senior executives are also expected to ensure their organisation's work and data agenda aligns with the Australian Government's Data and Digital Government Strategy (the Strategy).

The Strategy plays a central role in the Commonwealth Data Ecosystem and establishes the Australian Government's vision to deliver simple, secure and connected public services for all people and business through world class data and digital capabilities by 2030.

The Strategy provides the overarching context within which Government entities are expected to drive their data and digital operations. The Strategy includes the Australian Government's commitment that all APS agencies will appoint a senior leader with responsibility for their organisation's data. In this context, CDOs play a critical role in

facilitating their agency's alignment with the Strategy and engagement in the Commonwealth Data Ecosystem.

The Strategy also includes other Government commitments about how Government entities should manage and use their data, including that all Government entities:

- maximise value from data by:
    - making non-sensitive data open by default in compliance with relevant laws and appropriate privacy, security and ethical controls for sharing sensitive data;
    - sharing data between themselves, with state and territory governments, and with other users where appropriate and in accordance with appropriate agreements;
    - collecting and analysing data to assess whether policies and services are achieving their intended purpose and are being implemented in the best possible way;
    - harnessing analytical tools and techniques (including machine learning and artificial intelligence) to predict service needs, improve user experience, support evidence-based decisions and gain efficiencies in agency operations;
    - continuing to invest in new enabling technologies and streamlining governance and data sharing processes to allow greater access to timely and accurate data;
    - building partnerships and sharing data across the APS and with state and territory governments, and the private sector and non-government organisations; and
    - fostering a culture of data innovation.
- manage data as a valuable national asset by:
    - educating their staff on the importance and appropriate use of data;
    - embedding infrastructure maintenance plans into ICT schedules, to ensure the integrity and protection of data;
    - adopting best practice data collection and use to create data assets that support policy development and decision making;
    - adopting an organisation specific plan for using data, including identification of data assets, to achieve their organisational objectives;
    - incorporating appropriate data management and stewardship approaches, including identifying roles with specific responsibilities for these functions; and
    - embedding data quality standards into all data asset management functions, focusing on the key categories of data quality including accuracy, completeness, auditability, consistency, and timeliness.
- connect data, digital and cyber security by continuing to protect individual privacy and maintain security of sensitive information when expanding data capability and sharing.
- ensure technology is scalable, secure, resilient and interoperable, with new systems and infrastructure that supports data access and discoverability.

APS CDOs should also be aware of the other, non-data, accountabilities which may affect management of their organisation's data. For example, the:

- financial accountabilities derived from the *Public Governance, Performance and Accountability Act 2013* apply to the procurement of data;
- *Australian Government Charging Framework* applies where a fee is charged for access to data;
- *Privacy (Australian Government Agencies — Governance) APP Code 2017*, made under the *Privacy Act 1988*, assigns responsibilities to agencies to comply with the *Australian Privacy Principles*, enhance privacy capability and accountability, promote good privacy governance, and build community trust and confidence in the personal information handling practices of agencies. The code requires agencies to have a designated SES level Privacy Champion to ensure specific functions are carried out and a designated Privacy Officer;
- *Protective Security Policy Framework* outlines agency accountabilities for information security, including a requirement to comply with the *Information Security Manual;*
- *Archives Act 1983* outlines accountabilities for the management of records, including data records;
- *Freedom of Information Act 1982* includes accountabilities for the release of data in certain circumstances; and
- *National Statement on Ethical Conduct in Human Research* consists of ethical guidelines for research involving human participants, including ethical collection and use of data, but is only mandatory for research funded by the National Health and Medical Research Council.

2. Commonwealth Data Ecosystem

Finance has developed a model of the Commonwealth Data Ecosystem (Attachment A) with the aim of illustrating how the elements of the system relate to and complement each other. The representation of the ecosystem presents the data ecosystem divided into data 'practices' and recognises some key initiatives and activities underway within each practice area.

This section provides an overview of the different parts of the ecosystem and details some key initiatives relevant to CDOs. Some initiatives and activities are relevant to multiple data practice areas. The ecosystem is not intended to present the flow of data through its lifecycle.

2.1 Data and Digital Government Strategy

In December 2023, the Government released the Data and Digital Government Strategy (the Strategy) which outlines its vision to deliver simple, secure, and connected public services for all people and businesses through world class data and digital capabilities by 2030.

Finance and the Digital Transformation Agency (DTA) undertook extensive consultation with the community, the APS, industry, academia and state and territory governments to inform the Strategy. A summary of the feedback received through this process is provided in the What We Heard document. The Strategy is structured around five missions describing the key objectives and actions of the Australian Government to help realise the 2030 vision:

- **Mission 1 – Delivering for all People and Business**

  The Australian Government uses data and digital technologies to provide connected and accessible services centred around the needs of people and business.

- **Mission 2 – Simple and Seamless Services**

  The APS works as a single unified enterprise by using the right technologies, data, and analytics to simplify how they deliver for people and business.

- **Mission 3 – Government for the Future**

  The Australian Government is a leader in using new and evolving data and digital technologies in innovative ways to take advantage of opportunities and respond to emerging priorities.

- **Mission 4 – Trusted and Secure**

  The Australian Government will partner with people and business to ensure decisions and services are trusted, transparent and ethical, and support people's choices when engaging with public services.

- **Mission 5 – Data and Digital Foundations**

  The APS adopts the right capabilities, practices, standards, and culture and makes effective use of data and digital technologies to operate a seamless government.

Specific initiatives and measures to help realise the Strategy's 2030 vision are outlined in the Implementation Plan released alongside the final Strategy. The initiatives in the Implementation Plan will help guide the practical alignment of Government entities' activities with the Strategy.

2.2 Data by Design

Data by Design refers to an approach that ensures data collections and other issues are considered during the design phase of any system, service, product or process and also throughout the lifecycle. As part of taking a data by design approach, Government entities should consider how their activities align with and meet commitments under the Data and Digital Government Strategy.

As CDO you should:

- lead development and implementation of your organisation's data strategy and ensure it is consistent with the principles of data by design.

Strategic Data Investment Advice Function pilot

The Department of Finance is piloting a new function to provide data-specific advice to Government to support consideration of data-related investment proposals.

Finance will run the pilot through the 2024-25 Budget with an initial focus on identifying opportunities for Government to use or reuse existing data infrastructure. The function will involve Finance coordinating technical expert advice from relevant APS data agencies to complement its data-specific policy advice to be integrated within the existing Green Brief process.

There are no additional requirements on agencies at this stage. Finance will leverage existing Budget and Cabinet processes to analyse data-related proposals during the pilot.

The lessons learnt during the pilot will be used to develop a proposal for a permanent ongoing function for Government consideration.

For further information please contact: DataAdvice@finance.gov.au.

2.3 Manage

Data Management refers to the development, execution, and supervision of plans, policies, programs and practices that deliver, control, protect, and enhance the value of data and information assets throughout their lifecycles.

As CDO you should:

- set your organisation's standards and approach to data management and quality, including shared and open data; and
- manage enterprise level data-related risks and issues in line with your organisation's risk management policy.

The Foundational Four

The Foundational Four provides a clear starting point for simple, effective steps towards managing data. The primary aim of the *Foundational Four* is to provide agencies that are beginning their data journey with a starting place to improve their data practice. The framework is based on four elements of:

- **Leadership**: a senior leader is responsible and accountable for data across the agency (e.g. a CDO);
- **Strategy**: an agency has a clear vision and plan for using data to achieve objectives;
- **Governance**: mechanisms exist to oversee data management; and
- **Asset Discovery**: data assets have been identified and recorded.

For more information, please refer to the Foundational Four website.

Data Maturity Assessment Tool

Finance is leading development of a Data Maturity Assessment Tool (the Tool). The Tool is designed to provide Government agencies with a consistent approach to measuring their organisation's data maturity and monitor changes over time. The results will help agencies to understand their data capabilities, identify their capability gaps and areas for improvement, compare their progress against other agencies over time, and support cross-agency activities, such as data interoperability and data sharing.

The Tool is a key initiative in the Strategy's Implementation Plan and its completion will support progress towards the Strategy's vision. The Tool will also be an important source of whole-of-APS metrics used to inform reporting in the Strategy's Implementation Plan tracking progress towards a data-driven APS.

For further information please contact: DataPolicy2@finance.gov.au.

Framework for the Governance of Indigenous Data

The National Indigenous Australians Agency has developed an APS-wide Framework for Governance of Indigenous Data which aims to improve the accessibility, relevance, interpretability, and timeliness of government-held data for Aboriginal and Torres Strait Islander peoples.

The Framework will also explore the practical intersection between Australian Government objectives and those of the Indigenous Data Sovereignty movement in Australia.

NIAA developed the Framework in partnership with representatives of Australian Government departments, Aboriginal and Torres Strait Islander and other non-government representatives through Deputy Secretaries Data Group (DSDG) Sub-Committee on Governance of Indigenous Data.

The Framework was endorsed in-principle by the Secretaries Board in December 2023, with implementation efforts to start in 2024 under the oversight of the DSDG and the dedicated DSDG Sub-Committee. The Framework is expected to be released in the first half of 2024.

2.4 Access

This practice refers to the ability of people, businesses, academia and the APS to access the data they need to support their activities. The Australian Government generates a significant amount of data, the challenge is ensuring relevant groups can access this data. Initiatives under this data practice help overcome the challenge and improve data access.

As CDO you should:

- promote the release of data held by your organisation as open by default, prioritising high value data, and remove barriers to data sharing and release of non-sensitive data; and
- support staff in your organisation who work with and manage data, including assisting business areas to source external data.

Data.gov.au

Data.gov.au is the central source of Australian open government data. Anyone can access the anonymised public data published by federal, state and local government agencies.

Open government data is a national resource that holds considerable value for growing the economy, improving service delivery and transforming policy outcomes. In addition to government data, the platform also hosts publicly funded research data and datasets from private institutions that are in the public interest.

The Strategy includes the Australian Government's commitment that all government entities make non-sensitive data open by default in compliance with relevant laws and appropriate privacy, security and ethical controls for sharing sensitive data.

For further information please see data.gov.au or contact: support@data.gov.au.

Data hubs

Various APS agencies have established data hubs which are a tool which facilitates access to data in specific areas. The most prominent data hubs are:

- **Digital Atlas of Australia** (Geoscience Australia)

  The Digital Atlas of Australia brings together, curates and connects trusted national datasets from across government into an interactive, secure, and easy-to-use online platform.

- **National Freight Data Hub** (Department of Infrastructure, Transport, Regional Development, Communications, and the Arts (DITRDCA))

  The National Freight Data Hub is working closely with industry and government to deliver a wide range of projects focused on current and emerging freight data gaps, and opportunities to make better use of data to support planning and decision making.

- **Regional Data Hub** (DITRDCA)

  The Regional Data Hub aims to be an effective online resource connecting regional Australians to information and data about their communities in a single, accessible, and searchable location.

- **National Waste and Resource Recovery Data Hub** (Department of Climate Change, Energy, the Environment and Water)

  The National Waste and Resource Recovery Data Hub houses and displays national waste and resource recovery data. It's designed to make data more accessible for industry, governments, and the public. New data and supporting information will be gradually added to the data hub, in consultation with industry and governments.

2.5 Data Architecture

Data Architecture refers to the blueprint for managing an organisation's data assets by aligning with organisational strategy to establish strategic data requirements and designs to meet these requirements.

As CDO you should:

- lead development, publishing and maintenance of your organisation's information architecture;
- oversee and coordinate data architecture and business intelligence;
- manage your organisation's enterprise data costs in line with budget allocations;
- lead development and continuous improvement of your organisation's enterprise data governance framework; and
- oversee development and deployment of your organisation's enterprise data and analytics platform, if applicable.

Australian Government Architecture

The Australian Government Architecture helps us to assess new and existing digital solutions by seeing how they "fit in" with what we already have, whether a new solution helps "fill a gap", or whether what we are currently using is no longer "fit for purpose" and needs to be retired. In this way, the Australian Government Architecture can be used as a decision-making construct that supports more informed digital investments.

2.6 Integrate

Data integration refers to the process of combining data from two or more sources at a unit level (for example, at an individual or business level). Integrated data assets hold a range of data that allow complex questions to be analysed, with new insights that are not available from a single data source. State and territory governments also undertake a large amount of data linkage work.

As CDO you should:

- set your organisation's standards and approach to data management and quality, including for shared and open data; and
- as your organisation's Data Champion, provide input to the Data Champions Executive group regarding data integration work (as applicable).

Person Level Integrated Data Asset (PLIDA)

The Person Level Integrated Data Asset (PLIDA) (previously called the Multi-Agency Data Integration Project (MADIP)) is a secure data asset which combines information on health,

education, government payments, income and taxation, employment, and population demographics (including the Census) over time.

The project is enabled through a partnership of agencies, comprising:

- Australian Bureau of Statistics
- Australian Taxation Office
- Department of Education
- Department of Health and Aged Care
- Department of Social Services
- Services Australia
- Department of Home Affairs.

These agencies are also the members of the PLIDA Board, which is responsible for the data asset's operation and strategic direction. PLIDA datasets are linked via the Person Linkage Spine, which is kept separate from the analytical content of the PLIDA. This approach enables efficient and high quality linkages while maintaining a high standard of privacy and security.

Business Longitudinal Analysis Data Environment (BLADE)

The Business Longitudinal Analysis Data Environment (BLADE) is an economic data tool combining tax, trade, business insolvency and intellectual property data with information from ABS surveys to provide a better understanding of the Australian economy and businesses performance over time.

Currently the BLADE contains data on all active businesses from 2001-02 to the most recent full financial year, sourced from:

- Australian Bureau of Statistics (ABS) Business Register
- Australian Taxation Office
- ABS Surveys
- Australian Securities and Investments Commission
- Intellectual Property Australia
- Department of Foreign Affairs and Trade.

The ABS is the accredited integrating Authority of the BLADE. Through this role the ABS collects and combines the data, provides access to authorised researchers, and protects privacy and keeps information secure.

ANDII and the NDDA

The Australian National Data Integration Infrastructure (ANDII) is being developed as the underlying infrastructure to deliver the National Disability Data Asset (NDDA).

There is substantial data integration work occurring within the Australian Government and in most state and territories but this can be time-consuming, and inefficient. The ANDII is a transformational national linkage and integration infrastructure that provides the step change from individual activities within the Australian and state and territory governments to a national approach to data integration.

The ANDII enables the delivery of the NDDA which will inform what services people with disability are accessing, including mainstream services, and will be able to provide evidence as to the efficacy of those services. The NDDA will help inform policy development in multiple policy areas, including health and employment.

The ANDII is being developed through collaboration with the Australian, state and territory governments. It is being governed by the ANDII board which will provide strategic oversight on the design, build, operation and evolution of ANDII, including further applications of ANDII beyond disability. The ANDII Board reports to the Data and Digital Ministers Meeting.

Population Health Research Network

The Population Health Research Network (PHRN) is a national collaboration that enables existing data from around Australia to be brought together and made available for important research. The PHRN was established in 2009 and implemented through the National Collaborative Research Infrastructure Strategy framework, an initiative of the Australian Government. State and territory governments and academic institutions have made significant cash and in-kind contributions to PHRN activities.

The PHRN also facilitates the linkage of data which is not related to Health.

National Integrated Health Services Information

The National Integrated Health Services Information (NIHSI) is a major national linked health data asset for health research and analysis.

The NIHSI comprises data on admitted patient care services (in public and private hospitals), emergency department services and outpatient services in public hospitals for all states and territories with the exception of Western Australia and the Northern Territory.

The NIHSI also includes data from the Medicare Benefits Schedule (MBS), Pharmaceutical Benefits Scheme (PBS), Repatriation Pharmaceutical Benefits Scheme (RPBS), Residential Aged Care services data, National Death Index (NDI) and Australian Immunisation Register (AIR) data will be included from early-2024.

Researchers will be able to use the data set to explore issues such as validation of the current treatment pathways for chronic disease management and care.

2.7 Analyse and Use

Analysis and use refer to the ability to draw useful information and insights from data. Evolving technologies such as artificial intelligence and machine learning are transforming this practice.

As CDO you should:

- promote opportunities for data to improve your organisation's business outcomes;
- oversee your organisation's analytics function, including data analytics and data science; and
- as your organisation's Data Champion, promote and/or implement innovative data related initiatives within your organisation and the APS, including advising business areas about how data can be used to support policy proposals before they are presented to Cabinet.

Agencies undertaking a high volume or complex data analysis should consider having a separate **Chief Analytics Officer** or **Chief Data Scientist** with accountability for data analytics and data science. However, in most agencies this can be part of a CDO's role.

Interim Guidance on the Use of AI

The DTA and the Department of Industry, Science and Resources have developed Interim Guidance on Government use of generative AI platforms, comprising four principles designed to ensure the responsible, safe and ethical use of generative AI by the APS.

Principle 1 – AI should be deployed responsibly

You should only use publicly available generative AI platforms in low-risk situations. According to the advice, use cases which currently pose an unacceptable risk to government include but are not limited to use cases:

- requiring input of large amounts of government data; or classified, sensitive or confidential information;
- where services will be delivered, or decisions will be made; and
- where coding outputs will be used in government systems.

Principle 2 - Transparency and explainability

The information provided by public AI tools is often not verified, may not be factual, or may be unacceptably biased. Users must question where this data comes from and be aware of the nature of the tool being used.

Principle 3 - Privacy protection and security

Inputs into AI tools should not include or reveal classified information, or personal information. All activities need to align with legislation and policies relating to

information and data (e.g. the *Privacy Act 1988*, and the Protective Security Policy Framework).

Government information must only be entered into these tools if it has already been made public or would be acceptable to be made public. Classified or sensitive information must not be entered into these tools under any circumstances.

Principle 4 - Accountability and human centred decision making

Generative AI tools must not be the final decision-maker on government advice or services. Accountability is a core principle for activities within the APS. As such, humans should remain as the final decision maker in government processes. Users may wish to use tools to brainstorm options or draft content but ensure that the options are reviewed by a human prior to use.

2.8 Data Sharing

Data Sharing refers to the process of facilitating the transfer of data from one place to another. This practice is particularly focused on data held by a government agency that is valuable to others in delivering their activities. Responsibly, securely and seamlessly sharing data helps drive economic value, innovation, improve services, and deliver better outcomes for Australians.

As CDO you should:

- promote the release of data held by your organisation as open by default, prioritising high value data, and remove barriers to data sharing and release of non-sensitive data;
- maintain an inventory of all data assets held by your organisation, including on which basis they can be shared or open;
- build and maintain positive relationships with your organisation's other senior leaders, and promote opportunities for data to improve business outcomes; and
- as your organisation's Data Champion, promote sharing of data across the APS.

Data Availability and Transparency Act 2022 Scheme

The *Data Availability and Transparency Act 2022* (DAT Act) establishes a new, best practice scheme for sharing Australian Government data – the DATA Scheme. The DATA Scheme is underpinned by strong safeguards and consistent, efficient processes. It is focused on increasing the availability and use of Australian Government data to deliver government services that are simple, effective and respectful; inform better government policies and programs; and support world-leading research and development. The National Data Commissioner is the regulator of the DATA Scheme.

The Office of the National Data Commissioner (ONDC) is responsible for streamlining how public sector data is used and shared to:

- promote greater use of public sector data;
- drive innovation and economic benefits from greater use of public sector data; and
- build trust with the Australian community around government's use of data.

The ONDC is working across the Commonwealth, including with other regulators such as the Office of the Australian Information Commissioner, to ensure Australia's data sharing framework is underpinned by a strong foundation of transparency, privacy and security.

There are three types of DATA Scheme participant:

- **Data Custodians** are Commonwealth Government bodies who are custodians/ stewards of public sector data. Data custodians do not 'opt-in' to the DATA Scheme – they are automatically participants unless prescribed in the DAT Act as an excluded entity
- **Accredited Users** are eligible Commonwealth, state and territory government bodies and Australian universities accredited to collect and use public sector data. These entities must apply under the accreditation framework to become an accredited user
- **Accredited Data Service Provider (ADSP)** can be eligible Commonwealth, state and territory government bodies, and Australian universities. Once accredited, ADSPs can provide complex data integration, de-identification and secure data access services to support data sharing under the Scheme. Eligible entities must apply under the accreditation framework to become an ADSP.

It is possible for a Commonwealth body to be all three types of participant. State and territory government bodies and Australian universities can be both Accredited Users and ADSPs.

Under the DATA Scheme, Accredited Users can request Australian Government data from a Data Custodian. An ADSP can be used to provide data services to support the data sharing project. For example, the New South Wales Department of Health can request data from the Commonwealth Department of Social Services and the Australian Bureau of Statistics may provide secure data access services to support the sharing. An ADSP must be used if the project involves complex data integration.

Dataplace is the digital platform ONDC is building for DATA Scheme participants and others to manage data requests and sharing agreements. The platform brings together those wanting to get access to Australian Government data (such as researchers and those working on public policy and delivering public services) with Commonwealth agencies who are the data custodians. The platform is also used by the National Data Commissioner to regulate the DATA Scheme. You can onboard to Dataplace to:

- apply for accreditation to be a data user under the DATA Scheme;
- apply for accreditation to be a data service provider under the DATA Scheme;
- request Australian Government data, including under the DATA Scheme;
- develop a data sharing agreement – a general or DATA Scheme data sharing agreement; and
- monitor and report on your data sharing activities – what data your entity is sharing, with who and for what purpose.

The ONDC has developed a Metadata Attributes Guide to aid agencies that are considering data inventory uplift work. The Guide is based on a 2021 Data Champions Network project which produced a set of 26 metadata attributes, comprising 10 core attributes and 16 additional attributes:

The core attributes are:

- Identifiers: The identifier of the data asset is specific and unique to the agency
- Title: The most common useful name by which the data asset is known
- Description: A descriptive statement of the data asset
- Point of Contact: The relevant contact for the data asset
- Access Rights: Specifies access to the data asset
- Security Classification: The security classification applied to the data asset as specified by the Australian Government Protective Security Policy Framework
- Data Custodian: The custodian is the agency who has the control of the data asset and has the authority for sharing and disclosure
- Keyword: Word(s) or terms that describe the data asset subject matter
- Resource type: The type of data asset being described
- Date Modified: The most recent date the data asset record was either created, changed, updated or modified.

The additional attributes and further guidance on the core attributes is available at the ONDC Metadata Attributes Guide.

The National Data Advisory Council advises the National Data Commissioner on ethical data use, community expectations, technical best practice, and industry and international developments. The Council comprises nine members from the Australian government, business and industry, civil society groups and academia.

Data Sharing Principles

The Data Sharing Principles represents a modern risk management framework adapted from the international best practice ‘Five Safes framework’. The Principles include five elements and controls can be set within each element to manage the impacts of strategic, operational, privacy, ethical, and security risks. The Principles are:

- **Project**: Is the project an appropriate project or program of work?
- **People**: Is the data made available only to appropriately authorised and qualified persons?
- **Settings**: Is the data shared, collected and used in an appropriately controlled environment?
- **Data**: Are appropriate protections applied to the data?

- **Outputs**: Is the output of the project the final output? If not, is the output reasonably necessary or incidental to creation of the final output?

For more information, please refer to the ONDC's Share Data page.

Intergovernmental Agreement on Data Sharing

In 2021, National Cabinet signed the Intergovernmental Agreement on Data Sharing enshrining a commitment of all jurisdictions to share public sector data by default, where it can be done ethically, lawfully, safely and securely. Recognising data as a national asset is key to delivering outstanding policies and services for Australians and making Australia a leading digital economy.

For more information, please refer to Finance's IGA on Data Sharing page.

2.9 Preserve and Destroy

The preservation and destruction of data refers to the actions taken to safeguard the long-term viability and availability of data or destroy it if retention beyond a certain time is undesirable.

As CDO you should:

- Ensure data is appropriately considered in your organisation's business continuity and disaster recovery plans and participate in crisis simulations and disaster stress testing.

Records Authority

A records authority is a legal instrument that allows agencies to make decisions about keeping, destroying or transferring Australian Government records, including data. Records authorities are issued by the National Archives of Australia to provide its permission for the destruction of temporary records, after minimum retention periods have been reached. Records authorities also identify which records should be retained as the national archives of the Australian Government.

For more information, please refer to the National Archives of Australia's Records authorities page.

Check-up survey

Check-up is the National Archives of Australia's information management survey. It is an online self-assessment tool designed to measure Australian Government agencies' maturity and performance in managing their information assets (records, information and data). The survey is submitted to the National Archives annually, with sign off by agency heads.

The National Archives analyses the survey data to measure the whole-of-government information management maturity. The findings inform our report to the Minister.

Check-up is structured to align with the National Archives' Information Management Standard for Australian Government and the Building trust in the public record policy.

Agencies complete the survey to understand their information management maturity and set priorities for improvement. The National Archives analyses the survey data to measure whole-of-government information management maturity. This provides an evidence base for practical information management advice; assessment of agencies' progress on implementing the Building trust in the public record policy; and planning for future service delivery including transfer, storage and preservation of the national archives of the Australian Government.

The survey is completed and coordinated by the person (or people) with responsibility for information management within an agency. It should be submitted by your Agency Head, unless there are exceptional circumstances, as agreed to by the National Archives.

The National Archives regards survey sign off by the recognised agency head as assurance that the survey has been completed accurately and accountably by the agency in accordance with governance responsibilities including the *Public Governance Performance and Accountability Act 2013.*

For more information, please refer to the National Archives of Australia's Check-up survey page.

Data Interoperability Maturity Model

The National Archives of Australia has created the Data Interoperability Maturity Model (DIMM) and the DIMM Assessment Tool to enable agencies to measure their data interoperability capabilities. Increasing organisations' data interoperability can reduce costs, streamline data sharing processes, and future proof the readability and accessibility of data.

The DIMM measures an agency's progression across five interoperability key themes:

- **Business:** operational maturity for producing, consuming and sharing data on a tactical level;
- **Security:** awareness of, and response to, the security risks and issues of data interoperability;
- **Legal:** legal support for data interoperability;
- **Semantic:** the data structures that enable the meaning of exchanged information to be understood by people and systems; and
- **Technical:** the technology that supports data interoperability, including computer systems and services.

The DIMM also assesses the organisation's information and data governance used to coordinate and drive data interoperability.

It can be used at every level of an organisation and can be applied to all data produced by an agency that has the potential to be integrated, exchanged or shared.

For more information, please refer to the DIMM website.

2.10 Trust, Ethics and Privacy

Data ethics refers to how we procure, store, manage, use, and dispose of data in ways that are aligned with principles such as fairness, respect, responsibility, integrity, quality, reliability, transparency, and trust. Agencies in the APS should demonstrate trustworthy behaviours and uphold individuals' privacy.

As CDO you should:

- establish an ethical framework for your organisation's collection and use of data, including use of artificial intelligence and other automation technologies;
- build and maintain public trust in your organisation's use of data;
- ensure compliance with relevant legislation and information management policies; and
- ensure data quality, privacy, safe access, discoverability, ethical sharing and usage arrangements, including use of appropriate metadata.

The Privacy (Australian Government Agencies – Governance) APP Code under the *Privacy Act 1988* requires agencies to have a designated SES level **Privacy Champion** to promote a culture of privacy that values and protects personal information within an agency and a designated **Privacy Officer** who is the first point of contact for privacy matters within an agency, and is responsible for ensuring day-to-day operational privacy activities are undertaken.

Data and Digital Ministers' Meeting – Trust Principles

The Data and Digital Ministers' Meeting (DDMM) Trust Principles help ensure government use of data and digital technology is centred around better outcomes for citizens and business. The figure below identifies the four principles eight related commitments.

2.11 Security

Data Security refers to the processes that ensure data privacy and confidentiality are maintained, data is not breached, and data is accessed appropriately. The large volumes of sensitive information held by government make security critical to upholding the public's trust in the Government's use of data.

As CDO you should:

- work with other senior leaders in your organisation to ensure data security and protection, including safe storage and confidentiality; and
- work with the Australian Government's Cyber Security Co-ordinator as needed to meet obligations under the 2023-2030 Australian Cyber Security Strategy.

Chief Information Security Officers play a key role in ensuring the alignment of your organisation's cyber security and business objectives.

2023-30 Australian Cyber Security Strategy

The priority areas of the new Strategy will enhance Australia's collective cyber resilience, build capability to counter cyber-attacks and lift cyber security in our region; thereby helping Australian citizens and businesses protect themselves from cyber threats, and developing our national cyber resilience so we can bounce back quickly from cyber incidents.

For more information, please visit the Australian Cyber Security Strategy website.

Protective Security Policy Framework

The Protective Security Policy Framework (PSPF) is administered by the Department of Home Affairs and sets out the Government's minimum policy standards across 16 policies and supports entities in their:

- security governance
- information security (polices 8-11, below)
- personnel security, and
- physical security.

The PSPF applies to non-corporate Commonwealth entities subject to the PGPA Act to the extent consistent with legislation. The PSPF represents better practice for corporate Commonwealth entities and wholly-owned Commonwealth companies under the PGPA Act.

Entities must report on their maturity on each of the 16 PSPF policies to their portfolio minister and the Department of Home Affairs each financial year, and summarise their risk environment and security capability and identify key risks to the entity's people, information and assets.

By following PSPF policies 8 and 9, entities can ensure that data is correctly handled and shared.

- **PSPF policy 8 –Classification system**: outlines entities' responsibility to identify the information they hold, assess the security classification of this information and take appropriate steps to protect this information based on its level of value, importance and sensitivity.
- **PSPF policy 9 – Access to information**: details security protections that support the timely, reliable and appropriate access to Australian Government information, and requirements for sharing information and resources with external stakeholders. This includes the need-to-know principle, security clearances and temporary access arrangements to classified information. It also details requirements for managing access to information systems that hold security classified information.

PSPF policies 10 and 11 outline requirements for entities' cyber security and ICT settings.

- **PSPF policy 10 – Safeguarding data from cyber threats**: requires entities to mitigate cyber threats by implementing the following mitigation strategies from the Australian Signals Directorate's *Strategies to Mitigate Cyber Security Incidents*, and consider implementing the remaining strategies to achieve an acceptable level of residual risk for the entity.
    - application control
    - patch applications
    - configure Microsoft Office macro settings
    - user application hardening
    - restrict administrative privileges
    - patch operating systems
    - multi-factor authentication
    - regular backups.
- **PSPF policy 11 – Robust ICT systems:** requires entities to ensure the secure operation of their ICT systems to safeguard information and the continuous delivery of government business by applying the Information Security Manual's principles during all stages of the lifecycle of each system.

2.12 Capability and Culture

Data capability and culture refer to efforts across the APS to increase in-house data skills and develop a culture of using data to drive policy objectives and evaluation.

As CDO you should:

- foster the creation of a data-driven culture in your organisation that harnesses the value of enterprise data assets to inform decision-making;
- build capability of other CDOs (e.g. participate in cross-agency recruitment panels, mentor new CDOs, share knowledge);
- build and maintain your organisation's data literacy and specialist capabilities, including analytics;
- support professional data capability uplift in your organisation and across the APS;
- as your organisation's Data Champion, provide input to the Data Champions Executive group regarding potential opportunities to collaborate across the APS on common data collection, management and use issues, as well as opportunities to improve APS data workforce capabilities and data literacy; and
- as your organisation's Data Champion, establish and maintain a network of change agents across your organisation.

Agencies may choose to appoint a **Chief Information Governance Officer** who is responsible for establishing and maintaining an enterprise-wide culture for an accountable and business-focused information management environment. Often this function can be performed by the CDO or **Chief Information Officer**.

APS Data Profession Stream

The APS Data Profession (the Profession) aims to improve the attraction, development and retention of data talent in the APS workforce, through better knowledge sharing, identification of best practice, senior leadership engagement and oversight and whole of APS collaboration. The approach will include:

- recruiting specialist data graduates, developing existing data capabilities and enabling mobility across data roles;
- establishing a Data Professional Network to share knowledge, expertise and better practice in the collection, analysis and reporting of data;
- oversight and championing by APS Senior Leaders; and
- collaboration across APS and state and territory government.

In 2023-24, the Profession will support and promote the capability elements of the priority projects endorsed by the Data Profession Program Board. The Profession will focus on uplifting data capability through initiatives such as formal learning pathways, micro-credentials and communities for peer-based collaboration and resource. Discussions have

commenced with universities around micro-credentials and other formal learning opportunities.

Project highlight - Data job role personas

In December 2022, the APS Data Profession released an initial suite of four data job role profiles for four key data roles, covering data analyst, data manager, data scientist and data engineer, and two specialisation roles: geospatial analyst and statistician.

The intention of releasing these role descriptions is to develop a universal understanding of data professional roles, capabilities and alignment within the APS.

In October 2023, the APS Data Profession commenced work to expand the data job roles to include a further six personas, comprising: data governance officer, data steward, data project manager, data/metadata specialist, data architect and data translator. This are due to be published December 2023.

Further information about the personas can be found on the Data job role personas website.

The Profession also engages with the Graduate Data Network to identify how they can work together for mutual support and has a close connection with the Data Champions Network.

The Profession is open to all government employees with an interest in learning more about data and working with it. The APS Data Profession caters to emerging and existing data specialists, sophisticated data users and producers through knowledge sharing, peer-based learning and career development opportunities.

It aims to lift the data capability of the APS workforce through defining data capabilities, increasing diversity and mobility of people in data roles, and creating career pathways and development opportunities. The Profession aims to ensure the APS workforce can attract, develop, and retain the data capabilities required to harness the unprecedented growth in the availability and value of data.

Other APS Data Profession Stream projects underway include:

- Curated Learning Offerings;
- APS Data Capability Framework – review and self-assessment tool;
- EL2 Data Leadership Course; and
- Graduate Data Modules.

For more information on the APS Data Profession, please contact the ABS at data.profession@abs.gov.au.

3. Data Governance Groups and Communities

The Department of Finance is responsible for whole-of-Government data policy. This function is performed by the Data Policy section.

The Government data governance landscape consists of governance bodies which provide advice that feeds into the development of government data policies and help to coordinate and provides oversight of data initiatives and frameworks across agencies. It also consists of several governance groups which facilitate collaboration across jurisdictions. An organisation chart of the Government data governance landscape is available at Attachment B. The individual groups are discussed in further detail below.

3.1 Data and Digital Ministers' Meeting

Data and Digital Ministers from all Australian jurisdictions meet quarterly to drive cross-government collaboration on national data and digital priorities. Membership comprises data and digital Ministers from each of the Commonwealth, states and territories, as well as New Zealand. The chair of DDMM is the Commonwealth Minister for Finance who is responsible for public data and related matters, and whole of government data and digital policy coordination. The DDMM is supported by a Senior Officials Group comprising senior representatives from state, territory and New Zealand governments with responsibility for data and/or digital matters.

The DDMM oversees development of Australia's public data and digital capability, including through national alignment (e.g. working to a shared vision and common standards), harmonisation (e.g. sharing information to minimise duplication) and interoperability (e.g. Commonwealth and state-based systems can work together).

The DDMM is responsible for progressing three strategic priorities:

- delivering a seamless Digital ID experience for citizens
- reforming cross-jurisdictional data and digital platforms, services and protocols
- transforming services around life events.

In 2021, National Cabinet signed the IGA on Data Sharing enshrining a commitment of all jurisdictions to share public sector data as a default position. The DDMM is responsible for implementing the IGA including through a six-monthly National Data Sharing Work Program.

In 2022, National Cabinet tasked the DDMM with '*delivering government services fit for the digital age, including through implementing a federated ecosystem of digital identities and identifying opportunities to deliver seamless government services across jurisdictions*.' DDMM is the primary governance mechanism for delivering a national economy-wide system that provides Australians with a voluntary, secure, convenient and inclusive way of proving their identity online.

Other key priorities are:

- supporting the National Plan to End Violence against Women and Children 2022-32 through better data sharing in consultation with Women and Women's Safety Ministers;

- establishing and implementing a nationally consistent approach to the assurance of the use of artificial intelligence in government;
- strengthening cyber security and identity resilience; and
- improving digital inclusion of First Nations Australians in line with the National Agreement on Closing the Gap.

The DDMM Terms of Reference and Communiques are available here. For more information, please contact the DDMM Secretariat at DDMM@finance.gov.au.

3.2 Secretaries Digital and Data Committee

The Secretaries' Digital and Data Committee (SDDC) is a sub-committee of the APS Secretaries' Board. The purpose of the SDDC is to provide strategic leadership to promote an APS enterprise approach to the planning, coordination, investment, assurance, and delivery of trusted and secure digital and data capabilities across government.

There are two permanent SDDC sub-committees, the:

- Deputy Secretaries Data Group with responsibility over the APS data ecosystem; and
- Digital Leadership Committee with responsibility over the APS digital ecosystem.

The SDDC Terms of Reference can be found at Attachment C. For more information on the SDDC, please contact the DTA Secretariat at secretariat@dta.gov.au.

3.3 Deputy Secretaries Data Group

The Deputy Secretaries Data Group (DSDG) is responsible for maintaining oversight over the APS data ecosystem and providing advice to the SDDC. DSDG members champion a whole-of-government approach to promote innovation in the use of public sector data for administration, policy development, service delivery, and regulatory functions.

In 2023, the DSDG is focussing on:

- supporting improved management and use of data by Australian Government agencies and take a whole of government approach to progressing strategic public data opportunities;
- providing guidance and leadership for development of a Data and Digital Government Strategy;
- embedding a culture of data sharing by default within the Commonwealth and between Commonwealth and jurisdictions;
- advising on and facilitate agency partnerships outside of the Australian Government to support data policy objectives, including improved access to and use of data; and
- providing governance and oversight of commissioned data bodies.

The DSDG Terms of Reference can be found at Attachment D. For more information on the DSDG, please contact Finance at dsdg-coord@finance.gov.au

3.4 Data Champions

The Data Champions Executive (DCE) and the Data Champions Network (DCN) operate with a collaborative and APS-wide approach, and promote efforts to support, align and work together on specific work program initiatives.

The DCE is a strategic decision-making group providing stewardship for data strategy matters at a whole of APS level. The DCE comprises Chief Data Officers or equivalent from invited policy and service delivery agencies, as a strategic decision-making group providing stewardship for data strategy matters at a whole of APS level.

The DCE's role is to:

- contribute to the design and implementation of the APS-wide strategic data agenda, such as:
    - supporting development and delivery of a Data and Digital Government Strategy
    - supporting data capability and literacy uplift through the Data Profession
    - delivering projects agreed by the DSDG;
- identify and prosecute opportunities to collaborate across the APS on common data management and use issues; and
- deliver strategic advice and messaging to the broader DCN.

The DCN is an APS-wide community of data-focussed APS officials who share information, showcasing best data practices across the APS, and provide a communication channel for data related matters. DCN members' views and feedback on matters of strategic importance will feed into DCE decisions. The DCN comprises senior leaders in APS organisations acknowledged as the key internal contact point to be connected in with the APS-wide data agenda.

Each year, the DCN assembles a series of working groups to complete projects aimed at driving progress on a specific shared issue on the data agenda and commissioned by the DCE. These annual DCN projects are a critical source of new products and research to support agencies and the Government progress the APS data transformation. The 2023 projects are outlined in the box below.

All DCN members are expected to:

- promote use, sharing and re-use of data within their organisations and across the APS;
- promote and/or implement innovative data related initiatives, in line with identified strategic priorities, within the organisation and the APS; and
- provide input to the DCE regarding potential opportunities to collaborate across the APS on common data collection, management and use issues, as well as opportunities to improve data workforce capabilities and data literacy across the APS.

The Data Champions Terms of Reference can be found at Attachment E. For more information on the Data Champions Network and Executive, please contact Finance at datachampions-coord@finance.gov.au.

2023 Data Champions Network Projects

The DCN contributes to the design and implementation of an APS-wide strategic data agenda. The DCN, through working groups set up through agency nominations, undertakes a rolling program of project work to investigate key areas of interest for the Government's data agenda. Previously, the DCN has been tasked to deliver projects on topics such as metadata and interoperability, understanding data sharing and the governance of indigenous data. In 2023, the Data Champions Executive commissioned several whole-of-government projects to address priority issues. These projects largely build upon the findings and recommendations arising from previous DCN projects and align with other data initiatives occurring across the APS.

Data Maturity Project

The project will build on the release of the APS Data Maturity Assessment Tool (the Tool) developed by Finance with oversight from the DCE in mid-2023. The project will focus on supporting agencies in effectively responding to the release of the Tool and identifying actions for agencies to improve their data maturity based upon their assessment results. The project will contribute to tracking individual agency and whole-of-APS data maturity over time and across the data lifecycle, and creating an evidence base to support future policy and initiatives to respond to challenges in agencies' and APS data maturity. The project will align with the Government's APS reform priority to uplift data capability within agencies and across the APS as an enterprise. The project will also complement existing initiatives such as the Data Availability and Transparency Act Scheme accreditation and the National Archives of Australia's Check-up Survey.

Project Lead: Australian Bureau of Statistics.

Data Governance in Practice

The project will develop practical guidance to assist agencies implement effective data governance across data lifecycle. The project will build upon the recommendations of the 2022 Data Governance and Ethics project delivered through the DCN which identified ways to increase consistency in data governance across the APS. In particular, the project will work to establish data governance as a mandatory requirement for all APS agencies; develop clear guidelines for agencies on how to implement data governance; articulate clear roles and responsibilities for data governance and data management within and across agencies; and grow data governance expertise and capability within the APS.

Project Lead: Office of the National Data Commissioner.

APS Data Ethics Framework Project

The project will build on the findings of 2022 DCN Data Governance and Ethics project to develop a whole of government data ethics framework governing the collection, use and sharing of data and encourage consideration of ethical issues across the data lifecycle. The project will consider options for embedding the framework in the APS to ensure consistent ethical practices are engrained in decision making across agencies.

Project Lead: Australian Taxation Office.

3.5 Other Groups and Networks

There are several other Data Governance Groups which contribute to the Australian Government Data Governance landscape. These include:

3.5.1 DSDG Sub-Committee on Governance of Indigenous Data

The DSDG Sub-Committee on Governance of Indigenous Data was tasked with driving a coherent approach to Indigenous data initiatives across the APS, and responding to the Indigenous data sovereignty movement in Australia.

For further information on the DSDG Sub-Committee on Governance of Indigenous Data, please contact NIAA at GID@niaa.gov.au

3.5.2 Gender Data Steering Group

The Gender Data Steering Group was established in October 2022 to maximise the impact of the government's major data holdings as an evidence-base for gender equality policy and the development of a National Strategy to Achieve Gender Equality.

For more information on the Gender Data Steering Group, please contact PM&C at genderdatasecretariat@pmc.gov.au.

3.5.3 Location IDC

The Location IDC improves place-based policy, program and service delivery through strategic coordination and collaboration on location analysis, data and capabilities.

For more information on the Location IDC, please contact Geoscience Australia LocationIDC@ga.gov.au.

3.5.4 Commonwealth Data Integration Reference Group

The Commonwealth Data Integration Reference Group brings together senior APS executives with the necessary technical and policy skills, and sufficient breadth of view across the APS, to identify, discuss and champion the best way forward for new and existing data integration initiatives.

For more information on the Commonwealth Data Integration Reference Group, please contact Finance at datapolicy2@finance.gov.au.

3.5.5 Graduate Data Network

The Graduate Data Network (GDN) aims to empower graduates to advocate for better data use, analysis, and capability across the APS. Through a bottom-up approach, we want to encourage the effective use of data to drive policy, program and corporate delivery outcomes across the APS and for the benefit of all Australians.

The GDN includes graduates from both data specialist and non-specialist backgrounds, including policy, program and service delivery, legal, financial and other areas. We are united by the common desire to drive data literacy and more effective data use.

The three objectives of the GDN are to:

- **champion cultural change** – to improve how the APS uses data by identifying opportunities for improvement in various data related networks and programs;
- **empower graduates** – to provide graduates with the confidence to use data by building them a platform to discuss the opportunities and challenges of data analysis and use, and enable them to collaborate across agencies on initiatives and projects; and
- **collaborate with senior executives** – to manifest our grassroots approach to data related innovation by working with APS senior executive governance forums and stakeholders, such as the DSDG, DCN and the National Data Commissioner, to positively influence data culture in the APS.

For more information about the GDN, please contact the 2023 GDN Co-Chairs at:

Relevant Contact (2024 GDN Co-Chairs)	Email
Althea Rodrick	althea.rodricks@ato.gov.au
Ami Goeree	ami.goeree@homeaffairs.gov.au
Dean Quesada-Tchung	Dean.Quesada-Tchung@servicesaustralia.gov.au

3.5.6 International Data Policy Community of Practice

The International Data Policy Community of Practice is a forum for subject matter experts across the APS to engage in open discussion about the current and emerging global data policy landscape and help inform Australia's policy positions.

For more information on the International Data Policy Community of Practice, please email Finance at datapolicy2@finance.gov.au.

4. Contacts

Contact	Email
Data and Digital Government Strategy	
Data Policy team, Department of Finance	DataPolicy2@finance.gov.au
Digital Strategy team, Digital Transformation Agency	digitalstrategy@dta.gov.au
Data Governance Group Secretariats	
Data and Digital Ministers Meeting (DDMM) secretariat	DDMM@finance.gov.au
Secretaries' Digital and Data Committee (SDDC) secretariat	secretariat@dta.gov.au
Deputy Secretaries' Data Group (DSDG) secretariat	dsdg-coord@finance.gov.au
Data Champions Executive and Network (DCE and DCN) secretariat	datachampions-coord@finance.gov.au
Graduate Data Network (GDN)	
2024 Co-chair	althea.rodricks@ato.gov.au
2024 Co-chair	ami.goeree@homeaffairs.gov.au
2024 Co-chair	Dean.Quesada-Tchung@servicesaustralia.gov.au
Communities of Practice	
International Data Policy Community of Practice	datapolicy2@finance.gov.au
Data Maturity Assessment Tool Community of Practice	datapolicy2@finance.gov.au
DSDG Sub-Committee on Governance of Indigenous Data	GID@niaa.gov.au
Gender Data Steering Group	genderdatasecretariat@pmc.gov.au
APS Data Profession	data.profession@abs.gov.au

5. Additional Resources

Books

- Chief Data Officers' Playbook by Caroline Carruthers
- The Chief Data Officer Handbook for Data Governance by Sunil Soares
- DAMA Data Management Body of Knowledge (DMBOK)

Online resources

- The Chief Data Officer Playbook – IBM Institute for Business Value
- The Chief Data Officer in government: A CDO Playbook 2023 - Deloitte
- Capability, skills and professional development - NAA
- Chief data officers: Does your organisation need one? – Stuart Ridley, The Mandarin
- How to Evaluate - Australian Centre for Evaluation (ACE)
- Templates, Tools and Resources – ACE

Videos

- Data Governance, the CDO, and Building a Data-Driven Culture