Data Ownership in Government

INDEX

Data Ownership Model: executive summary

Data reuse within government is critical to more effective:

- policy development
- research
- digital services
- operations

The Central Digital and Data Office (CDDO) roadmap 2022 to 2025 committed to creating a Data Marketplace as a central place to understand how to access data across government in a legal, ethical and effective way.

However, government does not have a consistent framework around data ownership. The lack of a shared understanding of roles, accountabilities and responsibilities is most deeply felt around critical data which multiple public sector organisations may be reliant upon. This lack of shared knowledge prevents effective cross-government data sharing and, ultimately, the delivery of the government's commitments, including the Data Marketplace.

The proposed model defines 3 main government data ownership roles and their attached responsibilities.

These roles are:

- Data Owner - who has dedicated ownership for a logical grouping of data or data domain and in-depth knowledge of the overall business strategy in their data area
- Data Steward – who is responsible for day-to-day operational activities needed to support the data governance decisions made by data owners in their data domain
- Data Custodian – who is responsible for capturing, storing and disposing of data in line with the data owner's requirements

The model provides best practice guidance for departments on data ownership. It also sets minimum requirements to support a shared understanding of the roles, responsibilities and accountabilities for essential shared data assets. These critical data assets will be discoverable via the Data Marketplace. In addition, the ownership model allows for implementing consistent and standardised approaches to data ownership across government. The model has been subject to Alpha testing and is now in Beta phase after which it will be reviewed.

1. What is data ownership and why does it matter?

1. Data ownership does not deal with 'possession of data', it is about formalising the roles of people responsible for the management of data throughout its lifecycle. It establishes accountability for data access and usage, solving issues, iterating and versioning access and ensuring compliance with legislation, regulations and applicable guidelines.

2. Data is often cited as one of the most valuable assets of an organisation. It is also a liability with significant risks if not guarded. Like any asset, data must be protected and managed to be fit for purpose, used lawfully and ethically. It should also provide maximum value to the organisation and government. Data ownership behaviours are critical to ensure:

- compliance with regulations, legislation, policies and standards
- governing data controls are defined and implemented to manage risk, secure data and ensure data is fit for its intended purpose
- that data assets serve their intended business purpose and broader potential value to government
- data integrity so that people using the data have confidence that it is a reliable and trustworthy base from which analysis and business decisions can be made

3. Data governance maturity levels vary across government. Some organisations already have data ownership policies and implementation plans in place, whereas others are at the early stages of creating an enterprise-level model. This model helps public sector organisations understand the importance of data ownership behaviours and principles and ensure they have the policies and plans in place. Where public sector organisations already have ownership policies, it is an opportunity to assess, update where needed and reinforce the message about its importance.

4. Data reuse is critical to better research, policy development, digital services and operations. The Transforming for a digital future: 2022 to 2025 roadmap for digital and data published in June 2022 committed to creating a Data Marketplace (including a Data Catalogue, standards and governance models) to rival best practice across public and private sectors by 2025. This data ownership model applies to all data assets determined to be cross-government critical data assets for inclusion in the Data Marketplace. Guidance on defining and determining cross-government critical data assets is also available.

2. Who is this model for?

5. The importance and relevance of data ownership is not limited to data experts, but extends to all parts of government handling, producing, and using data. These include:

- senior leaders responsible for setting the strategy and direction for a government organisation or department, including those who do not have data-specific job titles

- people at all grades within government responsible for business processes, systems and services that involve data
- people responsible for risk management within public sector organisations
- data publishers and consumers who actively share data or plan to do so

6. The Data Ownership Model applies to UK government departments and arm's length bodies. These include:

- executive agencies
- non-departmental public bodies
- non-ministerial departments

7. Due to devolution, The Northern Ireland Executive, Scottish Government and Welsh Government can set their own approaches to data-sharing governance. Local government is not required to implement these principles and actions. There are many benefits to aligning data-sharing governance across the UK, and it is important that administrations of the UK continue to share effective practice and learn from each other.

3. What do we mean by data?

8. There are many different definitions of data. This model uses the definition provided within Chapter 1 of the National Data Strategy published by the government in September 2020:

> “When we refer to data, we mean information about people, things and systems. While the legal definition of data covers paper and digital records, the focus of this strategy is on digital information”

9. An area of potential confusion is the blurred lines between data and information. Data is often thought of as the "raw material of information" and information as "data in context". In reality, the two are intertwined and dependent on each other. Both data and information need to be managed effectively for value to be derived from it. The Data Ownership Model applies to the roles and accountabilities that specifically relate to data. In many organisations Information Asset Owners and Information Asset Managers are integral to their ownership model and the table at Annex A sets out how the roles relate to each other. Given the similarities between the roles of Data Owner and Information Asset Owner, some organisations may wish to combine them to clarify decision making. For further details on information assets and on the different information asset-related roles visit the specific guidance.

10. Each organisation will segment their data into logical groupings or data domains. Organisations will factor their business needs or areas of strategic interest when determining how they segment their data. This can be done in a number of different ways and there is no single right way to do this.

4. What are the government's overarching objectives for data ownership?

11. All central government departments and arm's length bodies must:

- have an enterprise-level data ownership model and supporting guidance in place that recognises that:
    - data ownership is the responsibility of the business and not the technology domain
    - the responsibilities of ownership are not exclusive to a single person and require close collaboration across organisational levels, including the delegation of responsibilities from the senior owners
- ensure that enterprise-level ownership policies include monitoring and reporting arrangements as part of their organisation's broader risk management practices (e.g. identify and counter any internal or external potential vulnerabilities and threats, which may be incorporated into the broader information asset risk management processes)
- ensure data assets are included in their organisation's asset registers and considered in their organisation's asset and knowledge asset management strategies
- consider where data assets may have value to wider government, society and the economy, and the protection and exploitation approaches required to realise it
- have named owners for all data assets determined to be critical at an enterprise level
- have a nominated accountable individual Data Owner for each data asset determined to be an Essential Shared Data Asset (as defined in published guidance)
- ensure every Essential Shared Data Assets has accurate metadata, which must include the name and roles of responsible Data Owners and Data Steward(s)
- include information about critical data assets (cross-government and enterprise-level) and any critical data elements they include within a central register or catalogue managed by the enterprise, linking the name of the owner with the asset
- ensure that each critical data asset (cross-government and enterprise-level) has an owner who understands what they are accountable for. Owners must ensure that stewards and process owners understand their responsibilities.
- ensure that where data is exchanged between public sector organisations and with other sectors it includes agreed roles, accountabilities and responsibilities in line with this model
- ensure the interoperability (the ability to exchange and use between different computer systems and software) of all its data, with its critical data prioritised, through common standards and practical steps such as data owners recognising the importance of maintaining good quality reference data. Where common data is used across business processes, services, products and systems, organisations should consider establishing an Enterprise Data Model (EDM) with data ownership agreed at a conceptual data model layer.

5. What principles should be promoted through data ownership?

12. The data ownership model should ensure that:

1. **data is recognised as a valuable resource** - data is potentially of great value to organisations and the wider digital economy and should be assessed whenever possible to support investment decisions, encourage data sharing and the potential to realise wider commercial and societal value through protection and exploitation. Data is also a liability as there is a risk of theft, loss or misuse.
2. **data is governed and managed throughout its lifecycle** - data must be handled in line with policies, standards and legislation, which includes:

    - The Data Protection Act 2018
    - The Public Records Act 1958
    - UK Government Licensing Framework[1]
    - The Digital Economy Act 2017
    - The Data Ethics Framework
    - The Data Sharing Governance Framework
    - The Data Maturity Assessment for Government
    - The Rose Book

3. **data is secure** - data is protected from unauthorised access, whether malicious, fraudulent or accidental
4. **data is defined for common interpretation** - data is clearly and consistently defined for common interpretation
5. **data is FAIR** - data is findable, accessible, interoperable (exchangeable and useable between different computer systems and software) and reusable
6. **data is standardised** - common data standards are applied wherever possible
7. **data is fit for its intended purpose** - data is of the quality needed for its intended requirement
8. **data is authoritative** - data is shared from a qualified authoritative source wherever possible

6. What are the roles and responsibilities?

13. Industry best practice sets out 3 roles:

[1] The data ownership model relies upon the enabling effect of the Open Government Licence, which allows for re-use of Crown copyright and Crown database rights material produced by government. The administration of Crown copyright and database rights is delegated to The Keeper of Public Records at The National Archives by the Monarch, and cannot be assigned away from the Crown to third parties without approval.

1. **Data Owner** - a senior individual responsible for a logical grouping of data (e.g. areas of interest for an organisation such as a business process of domains such as customers, benefits or a service)
2. **Data Steward** - business expert(s) managing data in day-to-day operations
3. **Data Custodian** - individual(s) responsible per application or group of applications

14. For enterprise-level models, it's recommended the model include other executive leadership roles. These roles include (these roles may not be carried out by different people):

- Chief Data Officer
- Data Protection Officer
- Chief Technology Officer
- Chief Digital Officer
- Chief Information Security Officer
- Senior Information Risk Owner

15. For large and more complex organisations the role of Process Owner may be required. Where a data journey across the value chain might cross into multiple departments or be shared with other public sector organisations, and where additional processing may use or transform the data, it is also recommended that Enterprise Data Owners (EDO) are established. EDOs have responsibility for specific logical groupings of data or data domains (such as entities and attributes) to ensure a consistent and common approach across data assets within, and beyond the enterprise.

16. The EDO would define the data attributes, establish business rules around the validity of the data and set thresholds for others to follow. They might also define the conditions by which the data should be used. Process Owners must work closely with the EDO to ensure the integrity of the original data is not compromised in the process of transformation, enrichment and/or aggregation. In this type of arrangement, we would not necessarily expect the EDO to have accountability for the accuracy, security and protection of such data, outside the EDO direct sphere of influence along the end to end lifecycle. We would expect the EDO to ensure the necessary policies and standards are in place. In addition to their BAU roles, Process Owners would have responsibility for:

- Managing data risks;
- Enforcing data policies and standards to drive improvement for the data which their processes touch;
- Affirming business awareness to ensure all managers, staff and contractors understand their own area of responsibility in relation to data protection, security, quality and capability, and
- Providing assurance to Information Asset Owners (IAO)s/ EDOs that risks are managed and mitigated.

17. There are existing mandated roles for critical data and personal data that must be added into the model. The UK General Data Protection Regulation (GDPR) defines the role of a Data Controller as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of

personal data. Public sector organisations often decide that the organisation as a legal entity is the data controller for UK GDPR purposes. In the context of the GDPR, Data Owners are accountable for the quality, integrity, and protection of their data domain. Data Owners in partnership with their Data Stewards and the organisation's Data Protection Officer, Chief Data Officer, Chief Technology Officer, Chief Digital Officer, Senior Information Risk Owner and Chief Information Security Officer (where present) would cover the accountabilities of the data controller.

18. An important objective of data ownership is shifting the view of data as an asset to data as a product, which requires that government defines and proactively measures how and where data is actually used and adds value. Finding ways to define and measure value is an important part of the roles of data owners, stewards and custodians.

6.1 Data Owner[2]

What is a Data Owner?

19. Senior individuals with dedicated ownership for a logical grouping of data, and in-depth insights of the overall business strategy in their data remit. The person with overall accountability for the meaning, content, quality and distribution of a given set of data. By liaising with a team of operational Data Stewards, they are empowered to steer and ensure the data is fit for its intended purpose.

Why do we need Data Owners?

20. Data Owners act as the strategic points of contact for the data within their remit. Using their knowledge of data applications, they influence the strategic direction of data, approve changes to data, support data governance practices in their area of responsibility, and allow organisations to make faster and more responsive decisions around data to achieve business outcomes.

What are Data Owners accountable for?

21. Data owners have accountability for:

- understanding how their data is being used, who by and where, data lineage and flow of data, and whether it is controlled properly
- working with local business requirements to define centralised data definitions for their subject areas
- providing guidance and directions to data stewards to ensure definitions are managed and adopted consistently
- strategic data decisions and approvals around business requirements and modifications to their data

[2] See paragraph 14 for the exception where the role of Process/Service Owner may be required to actively manage and assure the security, protection and quality of data within their processes, with remaining risks being looked after by the IAO.

- ensuring appropriate identification, protection and exploitation of data assets for wider governmental, societal and economic value, in collaboration with the organisation's Knowledge Asset SRO where there is one[3]
- ensuring that agreed data definitions are maintained in the data catalogue through their data stewards
- ensuring that the quality of the data they are responsible for is known, considering all critical data users
- the management, monitoring and reporting of activities to improve their data through their data stewards
- ensuring security measures, in accordance with the organisation's policies, are in place to protect data that is in transit, data received, or data transferred to another organisation
- ensuring an appropriate retention schedule is in place outlining storage periods for all data (particularly personal data), which is reviewed regularly
- ensuring their data assets comply with legal requirements for archival, disposal and preservation
- limiting access to data (particularly personal data or data of significance to national security) to those authorised to do so

Who should they be?

22. Data Owners should have a position at the leadership level (recommended to be at senior civil servant (SCS) level). They need to be able to use their authority and knowledge of business strategies and processes underpinning the data to make decisions. They don't necessarily need to have a granular understanding of the data.

What skills and experience are required of a Data Owner?

Skills and experience expectations…	…so that the Data Owner is equipped to
Data literate, with a strong "Data mindset"	Quickly understand the benefits and the foundational components of data governance, so that they are informed to put the data governance strategy and framework into action
An experienced leader who has a proven ability to deliver results, drive transformation through the organisation and lead/manage projects, programmes and change initiatives	Lead, influence and persuade their colleagues to adopt the data governance framework, such that the data standards and workflows are adopted and the corresponding business value is unlocked

[3] https://www.gov.uk/government/publications/dao-0321-managing-public-sector-knowledge-assets

	Ensure relevant operational and governance reporting to show effective adoption and adherence, Ensure KPI's have been appropriately set and approved, Review and ensure any issues actions identified are remedied Remove barriers to support delivery of projects and business changes,
Has a strong understanding of data and its impact on the day-to-day business and the importance of maximising the value of data assets as as applicable to their data domain	Understand the benefits of data governance, and the nuances of how it translates into practical implications for the data as governed, managed and exploited within their data domain
A strong communicator, able to take complex ideas and communicate them effectively to a non-technical audience	Translate data governance concepts into tangible 'so-what' that prompt non-technical colleagues into action
Has the ability to drive change, challenge and deliver under tight and ambitious timescales	Embed data governance at pace, so that the organisation can deliver on the business programme timelines and milestone commitments
Experience in executing successfully within a matrix organisation	Navigate across the Functions and Business, Operations
A problem solver; restless & agile: lives and breathes implementation	Put theory into practice – ensure that the organisation's data governance framework doesn't sit on paper but rather shapes our people take action day-to-day

6.2 Data Steward

What is a Data Steward?

23. Data Stewards are responsible for day-to-day operational activities needed to support the data governance decisions made by Data Owners in their data domain. They are responsible for the implementation of policies, standards, and processes.

Why do we need Data Stewards?

24. Having operational points of contact with data expertise ensures all data-related policies and the relevant strategic directions are fully embedded and that sustainable data governance processes are set up consistently across the organisation.

What are Data Stewards accountable for?

25. Data stewards have accountability for:

- handling data governance queries and checking with the Data Owner for tactical guidance where needed
- facilitating data governance processes, including:
    - data access
    - data archival
    - data deletion
- facilitating data quality governance processes, such as:
    - monitoring
    - investigating
    - communicating
    - triaging
    - remediating
    - reporting
- reporting to the Data Owner and other forums on activities including:
    - compliance
    - issues
    - fixes
    - changes
- the curation, maintenance and implementation, of data standards and process documentation (e.g. business glossary) in the data catalogue
- creating processes, procedures and standards for their data domain that is aligned to any enterprise-level policy in place
- relationship management and understanding the data lineage/flow to understand impacts (upstream or downstream) of anything that may change
- communicating and contributing to the development, maintenance and implementation of agreed data standards and reporting measures
- working cross functionally with other data stewards sharing good practice and supporting resolution on cross cutting issues/risks
- working with Data Custodians to facilitate discussions around technical requirements and modifications related to data governance standards
- assist with periodic data maturity assessments

Who should they be?

26. Data Stewards should have a deep knowledge of the operational/business area they are responsible for including the policies, processes, rules and requirements. Their subject matter expertise alongside strong communications and collaboration skills ensure data flows smoothly.

6.3 Data Custodian

What is a Data Custodian?

27. Data Custodians are responsible for capturing, storing and disposing of data in line with the Data Owner's requirements for technical tools for data-provisioning and delivery of business requirements (inc. data governance). Working closely with the Data Stewards to ensure data quality by executing within their systems according to the rules and standards as approved and directed by the Data Owner.

Why do we need Data Custodians?

28. Data Custodians, working as direct partners to Data Stewards, operationalise data decisions and support data governance implementation within the tools they are responsible for.

What are Data Custodians accountable for?

29. Data Custodians have accountability for:

- assisting Data Stewards with technical and system-related queries, spotting and reporting data governance issues to the Data Steward and Data Owner and producing impact assessments for implementing system changes led by the data steward
- implementing any technical requirements according to data standards and rules within their systems and data types. For example, adding a character limit on a field
- providing guidance and advice to other technical teams to ensure standards and definitions are used
- implementing user access policies specified by the Data Owner, including the appropriate physical and technical safeguards to protect the confidentiality, integrity, and availability of the data asset
- ensuring that data quality is sustained during technical processing
- resolving data quality issues in partnership with Data Stewards
- ensuring that changes to data content and controls can be audited

Who should they be?

30. Data Custodians should be technical SMEs for the system containing their assigned data. They should have in-depth knowledge and expertise around the system and be able to provide guidance on how to design and execute technical activities related to data governance.

Data ownership in relation to merged datasets and data lakes/services

31. It is essential that accountabilities for data are clearly defined and attributed to individuals or institutions in all models where data is processed. Use cases which pose challenges to the traditional model of ownership of a data asset include:

- data merged/linked from different sources to become a new dataset
- data being drawn from different sources into a data lake from which analysis and insights are drawn and data repurposed for multiple needs
- data being held in a trust or a cooperative where an institution or individuals steward the use and potential repurposing of data in the interests of those it represents.

32. In these use cases, data is either effectively transferred to an individual, institution or platform for usage or consumed at source via an Application Programming Interface (API) or other methods, such as secure file transfers. In these scenarios the source Data Owner must agree to the conditions by which access to the data is provided. This includes transfer of ownership or retained ownership and how it will be managed, along with defining the decisions that stewards/custodians can make on behalf of data providers/users.

33. Where a data platform or service is involved, a new role of product or service owner is likely to be required with specific accountability for:

- developing and operating the platform/service
- compliant access and use of data service
- compliance of use of data within the terms and conditions of its provision agreed with the source Data Owner

7. Glossary

Chief Data Officer - a senior executive-level role with responsibility for the organisation's enterprise-wide data and information strategy, governance, control, policy development, and effective exploitation. The role combines accountability and responsibility for information protection and privacy, information governance, data quality and data life cycle management, along with the exploitation of data assets to create business value.

Chief Digital Officer - a senior executive-level role with responsibility for driving digital transformation within an organisation using the potential of modern online technologies and data.

Chief Information Officer - a senior executive-level role with responsibility for the organisation's information technology (IT) strategy and implementation.

Chief Information Security Owner - A CISO is a designated individual responsible for the security of information in electronic form. They should advise the Board on how best to exploit technology to deliver the organisation's strategic objectives, and provide strong strategic leadership for the organisation's IT community and its investment in technology. They will be responsible for a department's IT strategy, IT architecture, IT policies and standards, technology assurance and IT professionalism.

Chief Technology Officer - a senior executive-level role with responsibility for the organisation's technological infrastructure and ensures that these are in alignment with business goals.

Data Controller - defined under UK GDPR as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Governance - the exercise of authority and control (planning, monitoring, and enforcement) over the management of data assets.

Data Protection Officer - is a specified role defined in data protection law (UK GDPR). A DPO is a role within an organisation that works in an independent manner to monitor the organisation's internal compliance, inform and advise on its data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner.

Information Asset - An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and life-cycles.

Information Asset Owner - Named senior individuals responsible for each identified information asset (e.g. database or ICT system) at the appropriate business level within a Department/Agency.

May - to show approval

Personal data - any information relating to an identified or identifiable natural person.

Senior Information Risk Owner - board level executive with particular responsibility for information risk. The role is no longer mandated by the Cabinet Office in the structure set in the Government Security: Roles and Responsibilities guidance published in November 2018.

Shall - to show a requirement

Should - to show a recommendation

8. Legal and copyright notices

Annex A - Roles

Title	Responsibilities	Role
Information Asset Owner (IAO)	Accountable for the information assets created by the processes in their business function and any named logical groupings of data or data domains. They are responsible for assuring that all the data risks and issues are managed and addressed per policies, standards and controls and applied by the Data Owners/Process Owners.	Executive
Enterprise Data Owner (EDO)	Has delegated responsibility from the IAO for assuring that the logical groupings of data or data domains assigned to their area of work have the right domain data standards, policies, and controls defined and are available for any valid use case. However, EDOs are not accountable for the data sets.	Strategic
Data Owner/Process Owner	Accountable for data quality, management and controls in their process area. They are the business subject matter experts (SMEs) managing the operational aspects of data in their process area. They will lead or contribute to: ● data policies ● standards ● data quality rules ● participating in the governance forums ● granting or revoking data access for data consumers They assure IAOs/IAMs that their processes have integrity and data risks are managed.	Operational
Data Steward	Data stewards are responsible for day-to-day operational activities needed to support the data governance decisions made by data owners for the data assets they are accountable for. They are responsible for the implementation of policies, standards, and processes.	Operational
Information Asset Manager (IAM)	Has delegated responsibility from the IAO for the proper handling and management of information in their business area. The IAM will assure the IAO that information and assets are being managed effectively per this model. They will escalate issues and exceptions as quickly as possible.	Operational
Local Information Manager (LIM)	Has delegated roles by IAMs within their lines of business to be LIMs. These could be existing staff, for example, Security and Information Business Partner or KIM leads, or other existing staff. The LIMs are responsible for compliance checks of electronic and hardcopy information, ensuring IAR is completed, and managing assets against risk management plan.	Support
Data Custodian	Group or individual from CDIO or an outsourced supplier who is the custodian of the physical data environment and the tools to facilitate: ● data collection ● processing ● storage and retrieval ● access and use. For example 3rd party suppliers and CDIO	Support