Queensland Government Enterprise Architecture

Information management policy framework

Final

August 2017

V2.0.1

PUBLIC

Document details

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. **Security classification** | 1. PUBLIC | | | | | |
| 1. **Date of review of security classification** | 1. August 2017 | | | | | |
| 1. **Authority** | 1. Queensland Government Chief Information Officer | | | | | |
| 1. **Author** | 1. Queensland Government Chief Information Office | | | | | |
| 1. **Documentation status** |  | 1. Working draft |  | 1. Consultation release | 1. 🗹 | 1. Final version |

Contact for enquiries and proposed changes

All enquiries regarding this document should be directed in the first instance to:

Queensland Government Chief Information Office  
[qgea@digital.qld.gov.au](mailto:qgea@digital.qld.gov.au)

Acknowledgements

This version of the *Information management policy framework* was developed and updated by Queensland Government Chief Information Office and the Queensland Government Information Sharing Community of Practice.

Feedback was also received from a number of agencies, which was greatly appreciated.

Copyright

*Information management policy framework*

Copyright © The State of Queensland (Queensland Government Chief Information Office) 2017

Licence



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/). For permissions beyond the scope of this licence, contact [qgcio@qgcio.qld.gov.au.](mailto:qgcio@qgcio.qld.gov.au.) To attribute this material, cite the Queensland Government Chief Information Office.

Material that is not licensed under a Creative Commons Attribution 4.0 License is:

* Branding
* Referenced content in section 2.2.3 What is knowledge?
* Referenced domain definitions for domain IDs: IM-1, IM-1.5, IM-2.3, IM-2.5, IM-2.6, IM-2.7, IM-2.8, IM-3.2, IM-4.1, IM-4.2, IM-4.5, IM-4.6, IM-4.8, IM-4.9, IM-5, IM-5.1-5.6, IM-6.1, IM-6.2, IM-6.3, IM-6.4 -6.6, IM-6.8, IM-6.9, IM-6.10, IM-6.11, IM-6.12.

Information security

This document has been security classified using the Queensland Government Information Security Classification Framework (QGISCF) as PUBLIC and will be managed according to the requirements of the QGISCF.

Contents

[1 Introduction 4](#_Toc490741491)

[1.1 Purpose 4](#_Toc490741492)

[1.2 Audience 4](#_Toc490741493)

[1.3 Scope 4](#_Toc490741494)

[2 Background 5](#_Toc490741495)

[2.1 What is the Information management policy framework? 5](#_Toc490741496)

[2.2 What is information? 5](#_Toc490741497)

[2.3 How can the Information management policy framework be used? 6](#_Toc490741498)

[2.4 How is the Information management policy framework structured? 6](#_Toc490741499)

[3 Information management policy framework 8](#_Toc490741500)

[3.1 Information governance 9](#_Toc490741501)

[3.2 Knowledge management 10](#_Toc490741502)

[3.3 Information asset management 11](#_Toc490741503)

[3.4 Information access and use management 12](#_Toc490741504)

[3.5 Records management 14](#_Toc490741505)

[3.6 Data management 15](#_Toc490741506)

[3.7 Information security 17](#_Toc490741507)

[4 Examples of use 18](#_Toc490741508)

[4.1 Scenarios of use 18](#_Toc490741509)

[4.2 Queensland Government IM policy classification 27](#_Toc490741510)

[Appendix A Summary of changes 32](#_Toc490741511)

Figures

[Figure 1 Information management policy framework v 2.0.0, 2017 8](#_Toc484700683)

[Figure 2 Information management initiative scoping 19](#_Toc484700684)

[Figure 3 Intellectual property initiative scoping 22](#_Toc484700685)

[Figure 4 Open data initiative scoping 25](#_Toc484700686)

[Figure 5 Classification of Queensland Government policies and legislation to framework with blue indicating policy or legislation exists. 29](#_Toc484700687)

[Figure 6 Summary of changes to Information management policy framework 32](#_Toc484700688)

# Introduction

## Purpose

The Information management policy framework (IMPF) identifies and defines the various areas (domains) which contribute to effective information management across the Queensland Government.

The IMPF is not mandated nor is it a QGEA policy. It is a tool for departments to use that can assist with making sense of information management within their own areas. Departments who use this framework should do so under the guidance that this is not a ‘one-size fits all’ approach to information management and should be adapted as necessary to suit individual business needs.

## Audience

This document is primarily intended for:

* information governance bodies
* information management staff.

## Scope

This document provides definitions for all information management domains, except for information security. Information security is only covered at a high level, for domain definitions please refer to Annex A [ISO/IEC 27001:2013 Information technology - Security techniques – Information security management systems – Requirements (second edition).](https://portal.qgcio.qld.gov.au/initiatives/cyber-security-unit/supporting-tools-and-services/3722-iso27000-suite?lnk=QS0yLTM3MjItNg)

This document does not detail the process around information management. The [Information asset lifecycle guideline](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/information-asset-lifecycle-guideline)provides additional guidance for users around the typical phases of an information asset lifecycle and the recommended approach for managing the information.

# Background

## What is the Information management policy framework?

The IMPF is an organising framework, for establishing a common viewpoint and understanding of information management across the Queensland Government. It can be used as a tool to categorise information management activities, and can be used as the basis for undertaking gap analysis and discovering duplications.

## What is information?

Information includes data, information assets and knowledge. The terms data, information assets and knowledge are only used when specific reference is required.

### What is data?

The representation of facts, concepts or instructions in a formalised (consistent and agreed) manner suitable for communication, interpretation or processing by human or automatic means. Typically comprised of numbers, words or images. The format and presentation of data may vary with the context in which it is used. Data is not information until it is utilised in a particular context for a particular purpose.[[1]](#footnote-2)

### What is an information asset?

An information asset is an identifiable collection of data stored in any manner and recognised as having value for enabling an agency to perform its business functions, thereby satisfying a recognised agency requirement. The [QGEA Information asset custodianship policy (IS44)](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/information-asset-custodianship-policy-is44) contains additional guidance on information assets.

### What is knowledge?

A body of understanding that is constructed by analysis of information. Knowledge is often embedded within people and increased through interaction with other people and information. Knowledge has many facets:

* It can be highly personal and may be consciously or subconsciously understood. Knowledge resides in a person’s mind and may include aspects of culture or ‘ways of doing things’ (often referred to as tacit knowledge).
* It can be recorded as information in a document, image, film clip or some other medium.
* It can be considered as a component of an organisation’s asset base[[2]](#footnote-3).

Every organisation will have knowledge based on its accumulated business experience, as well as the individual experiences of every person with whom it is associated[[3]](#footnote-4). Capturing and exploiting knowledge remains a significant area of challenge for organisations.

### What is information management?

Simply put, information management is the term used to describe all activities concerned with the use of information in all its forms.

More formally, information management is the means by which an organisation plans, identifies, creates, receives, collects, organises, governs, secures, uses, controls, disseminates, exchanges, maintains, preserves and disposes of its information; as well as any means through which the organisation ensures that the value of that information is identified and exploited to its fullest extent.

The primary aim of information management is to ensure that the right information is available to the right person, in the right format and medium, at the right time.

### What are records?

Any recorded information created or received by an organisation in the course of their business or conduct of their affairs. A record provides evidence of activities. This is irrespective of the technology or medium used to generate, capture, manage, preserve and access those records[[4]](#footnote-5).

## How can the Information management policy framework be used?

The IMPF can:

* provide a basis at both the departmental and whole-of-government level to identify and prioritise requirements for additional information management policies, guidelines and tools by mapping current policy effort and identifying gaps or duplications
* organise whole-of-government information management policies, guidelines and tools by domain, making departmental requirements in a specific areas clearer and related assistance more accessible
* form a basis for a consistent information management vocabulary across Queensland Government.

Section 4 of this document provides examples of how the IMPF can be used across several information management activity scenarios.

## How is the Information management policy framework structured?

The framework represents information management policy domains at two levels of detail. Level 1 domains (see figure 1 and 2), are the high-level domains and are as follows:

* **Information governance** – focus on overall policy, planning, architecture and direction for information and information management
* **Knowledge management** – focus on an integrated approach to managing knowledge, to enable the extraction of extra value from our information, including building upon knowledge and making valuable connections
* **Information asset management** – focus on full lifecycle management of information as an asset and classifying it so it can be found and used
* **Information access and use management** – focus on sharing, licensing and use of information so information is easy to find and able to be exploited as widely as possible
* **Records management** – focus on ensuring legislative and regulatory requirements are met, to fulfil business needs, accountability requirements and community expectations.
* **Data management** – focus on the management, and maintenance of the data that underlies our information
* **Information security** – focus on confidentiality, integrity and availability of information in line with *ISO/IEC 27001:2013 Information technology - Security techniques – Code of practice for information security controls* (second edition). Departments should refer to [Annex A ISO/IEC 27001:2013 Information technology - Security techniques – Information security management systems – Requirements (second edition)](https://portal.qgcio.qld.gov.au/initiatives/cyber-security-unit/supporting-tools-and-services/3722-iso27000-suite?lnk=QS0yLTM3MjItNg) for information security related definitions.

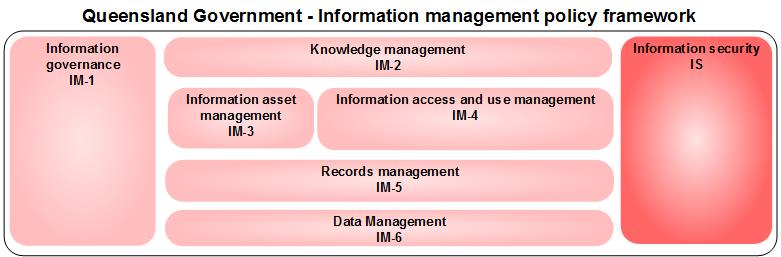


Figure 1 Information management policy framework level 1 domains

Each Level 1 domain contains several lower Level 2 domains (see figure 2) which define the elements of that (Level 1) domain in more detail where required. All domains are fully defined in section 3 of this document.

Domains with the IMPF may be associated with a whole-of-government policy, guidelines and other related documents. See section 4.2 of this document for an example classification of Queensland Government policies and legislation against the IMPF.

It should also be noted that many parts of the policy framework operate together. For example, the ability to truly obtain value from knowledge management, is dependent on sound data management, information asset management, information access and use management, and so on. The division into domains is not intended to give the impression that the areas can be dealt with entirely independently. In keeping with this, overlap between domains will occur, for example open data versus publishing and release, and open data versus data management. Similarly, data and information may become records from the moment they are created (for example, an entry in a database).

# Information management policy framework

The current version of the Information management policy framework is shown in figure 2 below.

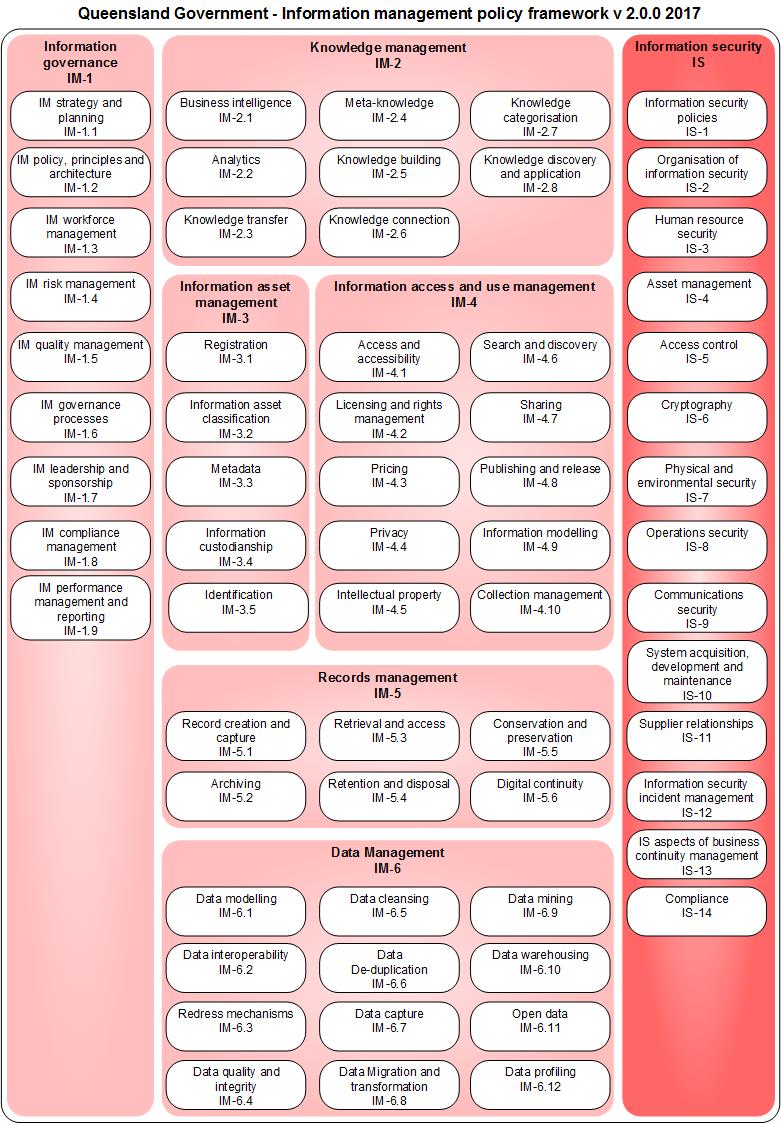


Figure 2 Information management policy framework v2.0.0, 2017

The remainder of this section provides definitions for each of the domains in the IMPF. Each domain has a unique domain identifier (ID), name and definition.

## Information governance

| Domain ID and name | Definition |
| --- | --- |
| IM-1 Information governance | Information governance is the system by which the current and future use of information and its management is directed and controlled.[[5]](#footnote-6) While all domains need to be governed the Information governance domain relates to the governance activities and not what needs to be governed |
| IM-1.1 IM strategy and planning | IM strategy defines the future strategic direction for the utilisation and management of information as a valued core strategic asset. Information and information management planning is concerned with ensuring that information and its management aligns with strategy and conforms to legislative and policy requirements. |
| IM-1.2 IM policy, principles and architecture | IM policy, principles and architecture provide direction and guidance with respect to information and information management activities, ensuring alignment with business requirements. |
| IM-1.3 IM workforce management | IM workforce management is concerned with the planning and maintaining of the information management workforce to meet current and future organisational needs. Information management capabilities should be taken into account during mainstream organisational workforce planning processes, and should inform strategies in relation to recruitment, skills development, advancement and succession. |
| IM-1.4 IM risk management | 1. IM risk management adapts the generic process of risk management (i.e. controls such as policies, procedures and practices to mitigate the effects of risk to an acceptable level) to information and information management.[[6]](#footnote-7) |
| IM-1.5 IM quality management | 1. IM quality management adapts the generic activities of quality management (e.g. establishing quality policies and processes to achieve quality objectives through quality planning, assurance, control and improvement) to information and information management.[[7]](#footnote-8) |
| IM-1.6 IM governance processes | 1. Information management governance processes are the specific processes that deliver information governance including the assigning of information governance roles and responsibilities. |
| IM-1.7 IM leadership and sponsorship | 1. Leadership is the ability to establish an information management vision and direction, to influence and align others towards a common purpose, and to empower and inspire people to achieve success. 2. Sponsorship is an important senior management role, whereby the sponsor is accountable for ensuring that information management is governed effectively and delivers the objectives that meet identified needs. |
| IM-1.8 IM compliance management | Compliance management reflects a department’s obligations to ensure compliance with, and appropriate management of all legislative policy and reporting obligations relating to information management. |
| IM-1.9 IM performance management and reporting | Performance management is the management and evaluation of information on the efficiency and effectiveness of whole-of-government direction, departmental business direction and service delivery to improve accountability of government, to information policy development and implementation and to create value to clients, stakeholders and the community. |

## Knowledge management

| Domain ID and name | Definition |
| --- | --- |
| IM-2 Knowledge management | Knowledge management is concerned with improving organisational outcomes and learning, through maximising the use of knowledge and capturing and applying learnings. |
| 1. IM-2.1 Business intelligence | Business intelligence is concerned with supporting better decision making by analysing internal and external information. |
| 1. IM-2.2 Analytics | Analytics is concerned with the application of rigorous statistical tools and techniques to a department’s information in order to improve decision making. |
| 1. IM-2.3 Knowledge transfer | Knowledge transfer is concerned with how tacit knowledge (i.e. knowledge that resides within a person’s mind) is transmitted among people.[[8]](#footnote-9) |
| 1. IM-2.4 Meta-knowledge | Meta-knowledge is knowledge about knowledge. |
| 1. IM-2.5 Knowledge building | Knowledge building can be defined as “the creation, testing, and improvement of conceptual artefacts.  Knowledge building refers to the process of creating new cognitive artefacts through establishing common goals, group discussions, and synthesis of ideas. These pursuits should advance the current understanding of individuals within a group, at a level beyond their initial knowledge level, and should be directed towards advancing the understanding of what is known about that topic or idea. The theory ‘encompasses the foundational learning, subskills, and socio-cognitive dynamics pursued in other approaches, along with the additional benefit of movement along the trajectory to mature education.’”[[9]](#footnote-10) |
| 1. IM-2.6 Knowledge connection | “Knowledge connection consists of collaborative learning, the transformation of tacit knowledge into explicit forms, and the documentation of best practices and lessons learned. Essentially it is ‘connecting people to content and connecting people to people’.”[[10]](#footnote-11) |
| 1. IM-2.7 Knowledge categorisation | “Categorisation is the process in which information management ideas and objects are recognised, differentiated and understood. Categorisation implies that objects are grouped into categories, usually for some specific purpose. Ideally, a category illuminates a relationship between the subjects and objects of knowledge. Categorisation is fundamental in language, prediction, inference, decision making and in all kinds of interactions.”[[11]](#footnote-12) |
| 1. IM-2.8 Knowledge discovery and application | Knowledge discovery and application is the process of extracting useful knowledge from information and data collections and using it within the organisation, such as to make decisions, perform tasks or enhance products and services.[[12]](#footnote-13)  See also data mining. |

## Information asset management

| Domain ID and name | Definition |
| --- | --- |
| IM-3 Information asset management | Information asset management is concerned with valuing and managing information assets with the same rigour as that applied to other strategic assets.  An information asset is an identifiable collection of data stored in any manner and recognised as having value to enable a department to perform its business functions, thereby satisfying a recognised department requirement. See [Information asset custodianship policy (IS44)](https://www.qgcio.qld.gov.au/products/qgea-documents/548-information/2632-information-asset-custodianship-policy-is44) for additional guidance on information assets. |
| 1. IM-3.1 Registration | Registration is the recording of an information asset in a repository for information management purposes for example, an information asset register. |
| 1. IM-3.2 Information asset classification | Systematic arrangement of information assets into groups or categories according to established criteria.[[13]](#footnote-14) Examples of established criteria for arranging information assets include among others the [Keyword AAA](https://www.records.nsw.gov.au/recordkeeping/resources/keyword-products/keyword-aaa), [Queensland Government Enterprise Architecture: Information Portfolio Framework](https://www.qgcio.qld.gov.au/products/qgea-documents/548-information/2746-information-classification-framework-definitions) and the [Queensland Government Information Security Classification Framework](https://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2417-queensland-government-information-security-classification-framework?lnk=QS0xLTI0MTctNA). |
| 1. IM-3.3 Metadata | Metadata is data about a particular information asset. Specifically, metadata is the contextual information about an information asset.[[14]](#footnote-15) A library catalogue record for a specific book is an example of a set of metadata (e.g. author, title, date, subject, location) that describe the information asset (the book). |
| 1. IM-3.4 Information custodianship | Information custodianship is concerned with the assigning of responsibilities to an individual or a group (the information custodian) for an information asset, who ensures that the information asset is appropriately identified and managed throughout its lifecycle and is accessible to appropriate stakeholders. |
| 1. IM-3.5 Identification | The process of identifying information assets of value to the enterprise to enable it to be managed.  Techniques for identifying information assets include:   * setting scope and agreeing on the qualities of an information asset * downstream analysis via business services and process (i.e. what information do we need) and/or upstream analysis via IT systems (i.e. what information is supported). * interviewing/conducting workshops with information custodians and system owners. |

## Information access and use management

| Domain ID and name | Definition |
| --- | --- |
| IM-4 Information access and use management | Information access and use management is concerned with how information is to be accessed, exchanged and used, by whom and on what terms. |
| IM-4.1 Access and accessibility | Access and accessibility is concerned with both:   * how access to government information is maximised for use and reuse * understanding how information may be accessed on a spectrum from closed to shared to open[[15]](#footnote-16) * ensuring that all reasonable steps are taken to minimise social, economic and geographic disadvantage to accessing information. |
| IM-4.2 Licensing and rights management | Licensing is concerned with determining and managing the rights of use of government information to be granted under a licence. An example is the Creative Commons licences which provides a method for specifying how information may be used lawfully. For the purpose of this framework, licensing includes rights management which protects information from unauthorised access or use.[[16]](#footnote-17) |
| IM-4.3 Pricing | Pricing is concerned with the transparent and consistent pricing of government information. |
| IM-4.4 Privacy | In the context of information management policy, privacy is concerned with how personal information is collected, managed and disclosed (including de-identification techniques) by government. This extends to an individual’s right to privacy and to access and amend their personal information. |
| IM-4.5 Intellectual property | Intellectual property covers the wide range of intangible property that is the result of investment in the creative and intellectual effort of an organisation’s various legal rights to protect the result of original and creative effort.[[17]](#footnote-18)  Intellectual Property includes copyright, the most common form of intellectual property owned or used by Queensland Government. |
| IM-4.6 Search and discovery | Search and discovery is concerned with the processes through which one searches, identifies and retrieves government information.[[18]](#footnote-19) |
| IM-4.7 Sharing | Sharing is concerned with sharing or exchanging of information between Queensland Government departments and with other organisations. |
| IM-4.8 Publishing and release | Publishing is concerned with assembling information, into a desired format and disseminating it to a wide target audience, generally the public. Examples of the output of publishing include a department website or a Government Gazette.  Release is concerned with the concept of administrative access to information and how it supports proactive disclosure of information,[[19]](#footnote-20) along with publication schemes and disclosure logs as required by the *Right to Information Act 2009 (Qld).* |
| IM-4.9 Information modelling | “Activities related to defining and representing the information requirements or landscape of the organisation, including the flow of information both internal and external to the organisation.”[[20]](#footnote-21) |
| IM-4.10 Collection management | In the context of this framework, collection management is concerned with managing a collection of information throughout its lifecycle. Examples of collections include:   * collections that are permanent in nature (e.g. archives) * collections that are specialist in nature (e.g. geological and botanical) * libraries * museums. |

## Records management

| Domain ID and name | Definition |
| --- | --- |
| IM-5 Records management | The field of management responsible for the efficient and systematic control of the [creation](https://www.forgov.qld.gov.au/glossary/create), receipt, maintenance, use and [disposition](https://www.forgov.qld.gov.au/glossary/disposal) of [records](https://www.forgov.qld.gov.au/glossary/records), including processes for [capturing](https://www.forgov.qld.gov.au/glossary/capture) and maintaining [evidence](https://www.forgov.qld.gov.au/glossary/evidence) of and information about business [activities](https://www.forgov.qld.gov.au/glossary/activity) and [transactions](https://www.forgov.qld.gov.au/glossary/transactions) in the form of records.[[21]](#footnote-22) |
| IM-5.1 Record creation and capture | 1. Record creation is the act of creating and [capturing](https://www.forgov.qld.gov.au/glossary/capture) a [record](https://www.forgov.qld.gov.au/glossary/records) to ensure actions or decisions are documented somewhere–this may be an email, file note, an entry in a database. Creating a record means you, or someone else in your organisation, can refer to it when needed. 2. Record capture is the saving or registering a [record](https://www.forgov.qld.gov.au/glossary/records) into your organisation’s [recordkeeping system](https://www.forgov.qld.gov.au/glossary/recordkeeping-systems) (whether hardcopy or [digital](https://www.forgov.qld.gov.au/glossary/digital-records)). This may mean registering the record into a recordkeeping system and assigning [metadata](https://www.forgov.qld.gov.au/glossary/recordkeeping-metadata) to describe it and place it in context, allowing for the appropriate management of the record over time. 3. This applies to all records regardless of [format](https://www.forgov.qld.gov.au/glossary/format-file-or-record) and any recordkeeping system, whether a dedicated [eDRMS](https://www.forgov.qld.gov.au/glossary/electronid-document-and-records-management-system-edrms-records-system) or a paper-based system to track records.[[22]](#footnote-23) |
| IM-5.2 Archiving | Archiving is the process of permanently preserving selected records that are no longer required for current business use.[[23]](#footnote-24) |
| IM-5.3 Retrieval and access | 1. Retrieval is the process of locating material or information in [storage](https://www.forgov.qld.gov.au/glossary/storage) and returning it for use.   Access is the right, opportunity, means of finding, using or [retrieving](https://www.forgov.qld.gov.au/glossary/retrieval) information.[[24]](#footnote-25) |
| IM-5.4 Retention and disposal | Retention and disposal is concerned with defining the temporary or permanent status, retention periods, disposal triggers, and consequent disposal actions authorised for classes of records.[[25]](#footnote-26) |
| IM-5.5 Conservation and preservation | Conservation is the direct intervention by a specialist on the structure or physical make-up of a damaged or at-risk document or [record](https://www.forgov.qld.gov.au/glossary/records) to ensure its survival without further degradation.  This is usually in the form of remedial treatments or repair on an individual basis. Conservation treatments use the least amount of intervention possible and may include [preservation](https://www.forgov.qld.gov.au/glossary/preservation-and-conservation), restoration, examination, documentation, research, advice, treatment, preventive conservation, training and education.  Preservation is the processes and operations involved in ensuring [records](https://www.forgov.qld.gov.au/glossary/records) are [stored](https://www.forgov.qld.gov.au/glossary/storage) and safeguarded from damage or loss of information. Information may be lost because of [obsolescence](https://www.forgov.qld.gov.au/glossary/technological-obsolescence), degradation, damage, and/or deterioration. This is irrespective of the [retention status](https://www.forgov.qld.gov.au/glossary/retention-status) of the records.  Preservation uses non-interventional measures that prevent or slow damage–mainly through protective and universal controls for storage, handling, environmental conditions, pest management, digitisation, disaster preparedness and response.[[26]](#footnote-27) |
| IM-5.6 Digital continuity | The ability to [access](https://www.forgov.qld.gov.au/glossary/access) and use [digital records](https://www.forgov.qld.gov.au/glossary/digital-records) through organisational, business and technological changes for as long as required. Ensuring long-term [access](https://www.forgov.qld.gov.au/glossary/access) to records is difficult due to:   * storage media deteriorating, and software, storage media, and hardware becoming obsolete * complexities associated with authenticity and integrity of [digital records](https://www.forgov.qld.gov.au/glossary/digital-records).[[27]](#footnote-28) |

## Data management

| Domain ID and name | Definition |
| --- | --- |
| IM-6 Data management | Data management is concerned with valuing and managing data as a strategic asset of government with the same rigour as that applied to other strategic assets. |
| IM-6.1 Data modelling | Data modelling is a method used to define and analyse the data requirements needed to support department processes and service delivery.[[28]](#footnote-29) |
| IM-6.2 Data interoperability | Data interoperability is the exchange of information that preserves the meaning and relationship of the data exchanged.[[29]](#footnote-30)  Data integration is the process of combining data residing at different sources and providing the user with a unified view.[[30]](#footnote-31) |
| IM-6.3 Redress mechanisms | Redress mechanisms provide transparent complaints and appeals processes to ensure data is maintained and of high quality.[[31]](#footnote-32) An example of a redress mechanism is the provision of a means for amending one’s personal information held by government. |
| IM-6.4 Data quality and integrity | Data quality and integrity is concerned with ensuring methodical data collection and practices to enhance quality, and integrity with respect to accuracy and completeness.[[32]](#footnote-33) |
| IM-6.5 Data cleansing | Data cleansing is concerned with detecting and correcting or removing corrupt or inaccurate data.[[33]](#footnote-34) |
| IM-6.6 Data de-duplication | Data de-duplication is concerned with the elimination of redundant data to reduce required storage capacity and establish a source of truth.[[34]](#footnote-35) |
| IM-6.7 Data capture | Data capture is concerned with the collection, possible manipulation and/or interpretation and storage of data. Data capture may be automated. Effective data capture can improve quality, coverage and reliability of data. |
| IM-6.8 Data migration and transformation | Data migration is concerned with transferring data between either storage types, formats or computer systems.[[35]](#footnote-36) Data transformation converts data from a source data format into destination data.[[36]](#footnote-37) |
| IM-6.9 Data mining | Data mining is the process of analysing data from different perspectives and summarising it into useful information – information that can be used to increase revenue, cut costs or both. Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases.[[37]](#footnote-38) This practice is similar to data science. |
| IM-6.10 Data warehousing | “Data warehousing are systems used for reporting and data analysis, and are considered core components of business intelligence. Data warehouses are central repositories of integrated data from one or more disparate sources. They store current and historical data and are used for creating analytical reports for knowledge workers throughout the enterprise.”[[38]](#footnote-39) |
| IM-6.11 Open data | “Open data is data that anyone can access, use or share.”[[39]](#footnote-40) |
| IM-6.12 Data profiling | “Data profiling is the process of examining data available from an existing information source (e.g. a database or a file) and collecting statistics or informative summaries about that data.”[[40]](#footnote-41) |

## Information security

For domain definitions please refer to Annex A [ISO/IEC 27001:2013 Information technology - Security techniques – Information security management systems – Requirements (second edition)](https://www.qgcio.qld.gov.au/information-on/information-security/services/iso-27000-suite) (logged in users only).

# Examples of use

This section provides examples of how the IMPF could be used.

## Scenarios of use

The following are example scenarios of how the IMPF may be used by the Queensland Government including:

* scoping an initiative or activity
* identifying relevant policies and guidance; and
* collaboration opportunities.

### Scenario 1: Information management initiative

After undertaking an information management audit, an external auditor identified a number of high risk information management processes that require Department A’s attention.

To mature their information management practice, it was determined that several governance foundations first needed to be established or improved, such as:

* having a consistent view of information holdings
* identifying authoritative sources of data
* identifying sensitive data
* formalising information custodian roles and responsibilities
* determining minimum technical security requirements for sensitive data
* assessing the technical security of sensitive information holdings.

While Department A has an information asset register, the information contained is not accurate, with many assets defined and classified in an ad hoc manner.

Department A commences an activity to:

1. Determine a consistent approach to identifying, classifying and detailing information asset holdings.
2. Understand and verify the information held in key corporate solutions.
3. Gain formal acceptance by information custodians.
4. Understand and verify what information is exchanged between key corporate solutions.
5. Assess whether corporate solutions have the correct level of security applied in relation to the sensitivity of the information contained within.
6. Mitigate or treat any existing risks associated with how information is managed in key corporate solutions.
7. Develop a plan to improve the department’s information management maturity.

The Information Management team uses the IMPF to help understand the scope of the activity, including any governance and security requirements in the management of information assets.

Initially the team scope the activity identifying the relevant domains in the IMPF (see circled domains below in figure 3).

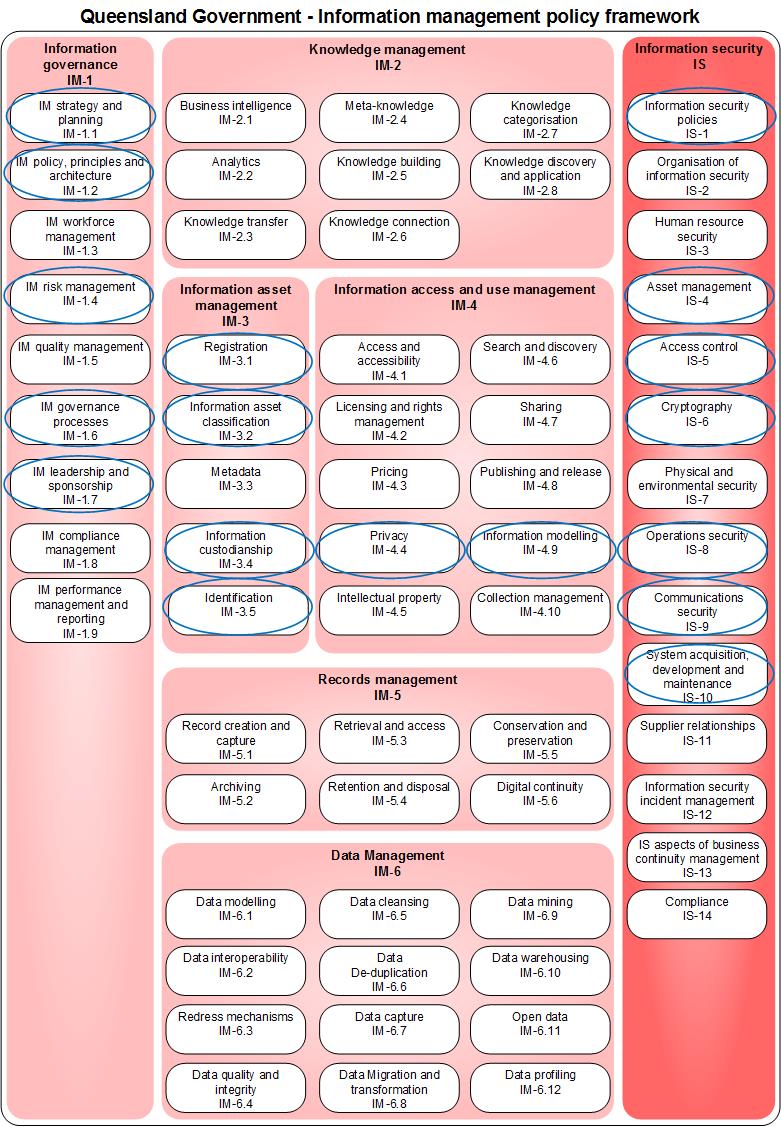


Figure 3 Information management initiative scoping

The table below breaks down the activities that occur in this initiative in each domain. It also demonstrates how relevant support is identified via the IMPF.

| Domain | Activity |
| --- | --- |
| IM-1.1 IM strategy and planning  IM-1.7 IM leadership and sponsorship | The IM team consults with executive and operational stakeholders to determine the desired state for information management. |
| IM-3.5 Identification | A process to identify information assets for management commences. This involves researching the corporate applications, interviewing staff and reviewing existing information asset registers. |
| IM-3.1 Registration | The existing information asset repository is updated. New entries are added and existing entries updated where appropriate.  The team identify that a related whole-of-government standard relates to this domain, the [ICT profiling standard](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/ict-profiling-standard-redirect). This standard provides minimum attributes for in scope information assets. The team ensure that these attributes are collected or updated. |
| IM-1.2 IM policy, principles and architecture  IM-3.4 Information custodianship | To help make decisions about each information asset, responsible custodians for each information asset are identified or confirmed. These details are also added to the register.  The team also define departmental materials that have been classified to this domain that can assist with briefing new information custodians on their roles and responsibilities. |
| IM-3.2 Information asset classification;  IM-4.4 Privacy  IS-4 Asset management | With the custodian of each information asset, security classification is reviewed or assessed using the [Queensland Government Information Security Classification Framework](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/information-security-classification-framework-qgiscf). |
| IM-1.2 IM policy, principles and architecture  IM-4.4 Privacy  IM-4.7 Sharing  IM-4.9 Information modelling | With key attributes in the information asset register completed, the team can then explore in more detail how information is exchanged between the key corporate applications and identify how that information is sourced. |
| IS-1 Information security policies  IS-4 Asset management  IS-5 Access controls  IS-6 Cryptography  IS-7 Physical and environmental security  IS-8 Operations security  IS-9 Communications security | With an understanding of each information assets’ information security classification and how they are used the team can review the security controls that are being applied.  The team review the applied controls are to an acceptable standard for the custodian and meet the [Queensland Government Information Security Classification Framework](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/information-security-classification-framework-qgiscf) and the [Australian Signals Directorate (ASD) Information Security Manual (Controls).](https://www.asd.gov.au/infosec/ism/) |
| IM-1.4 IM risk management  IM-1.6 IM governance processes  IS-10 System acquisition, development and maintenance | The team updates operational processes to ensure continued maturity in how information is managed. |

### Scenario 2: Intellectual property

Department B has recently been formed after a machinery-of-government change and is establishing a consolidated intellectual property (IP) register to record existing and assist with the management of new IP.

IP covers copyright, trademarks, patents, plant breeders’ rights, design, circuit layout rights and trade secrets. Copyright is the most common form of IP developed and released by Queensland Government departments. The department will be reviewing all its IP to determine whether it is suitable for public release and if so, what Creative Commons license could be applied. The department is committed to releasing public information under the least restrictive Creative Commons license as per the Queensland Public Sector Intellectual Property Principles.

The IP team utilise the IMPF to determine what other areas of information management practice may be relevant to the initiative.

The team identify that in addition to information access and use management there are several other areas such information security, information asset management and records management which are relevant in assessing IP for release. The department identifies it has mature information security classification processes that can assist with the release and licensing decision making process.

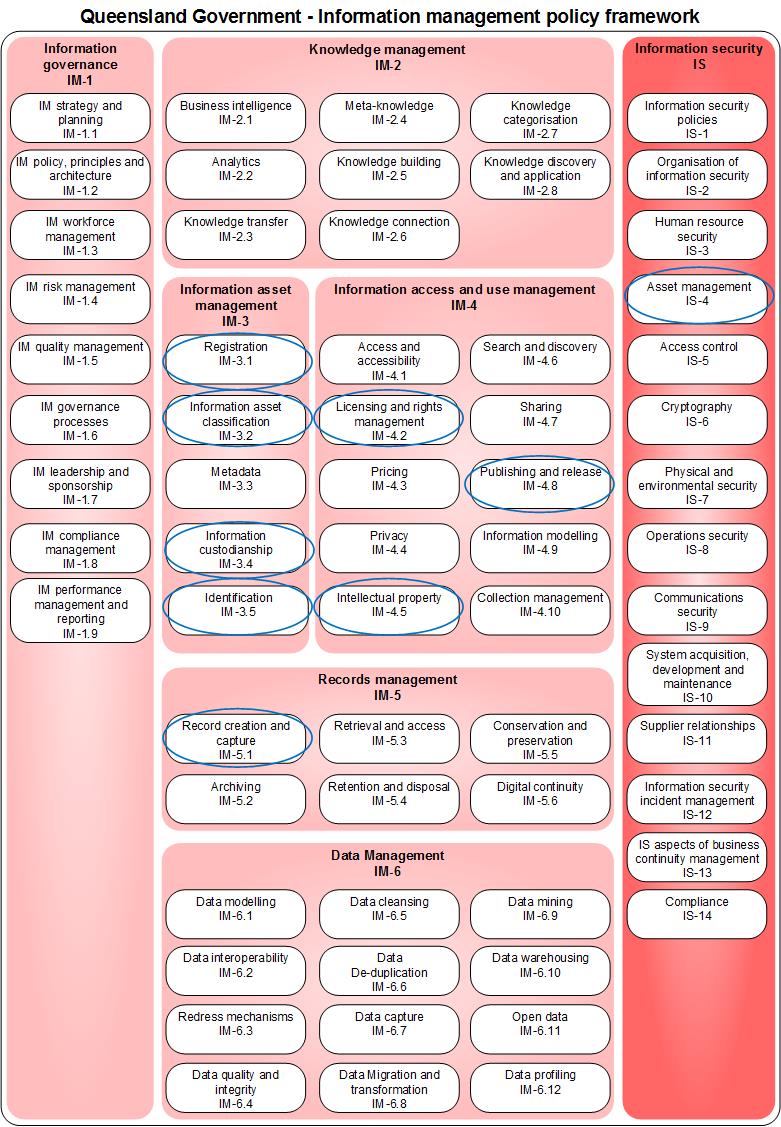


Figure 4 Intellectual property initiative scoping

The table below breaks down the activities that occur in this initiative in each domain. It also demonstrates how relevant support is identified via the IMPF as the department has classified its policies and guidance to the IMPF.

|  |  |
| --- | --- |
| Domain | Activity |
| IM-3.5 Identification  IM-4.5 Intellectual property | A process to identify IP assets that will be managed by the new department commences. This involves:   * researching and reviewing the IP registers of the departments in scope of the machinery of government change * working with staff to identify those that will be managed by the new department.   As the team have classified existing departmental and whole-of-Government policies to this framework they identify existing whole-of-government, departmental and Australian Government policy and guidance that can assist here including:   * the department’s IP policy, * [Queensland Public Sector Intellectual Property Guidelines](https://www.forgov.qld.gov.au/__data/assets/pdf_file/0024/182706/qps-ip-principlesfinal-v.2.pdf), * [Business Innovation and Improvement (BiiG) IP tool kit](http://biig.govnet.qld.gov.au/); and * Australian Government Intellectual Property Manual. |
| IM 3.2 Information asset classification | The identification and classification of information assets assists with identifying the scope, types use and functions of an department’s IP asset recorded within the register. It helps to facilitate the access and reuse of information and reduces any unnecessary duplication. |
| IM-3.1 Registration | As IP assets are identified for management they are registered by a team member in the department’s IP asset register within its recordkeeping system. New entries are added and existing entries updated where appropriate.  In the case of identified IP, the team member records the date of publication (if applicable), creator, 3rd party materials/resources included in the IP, custodianship, security classification and where applicable licensing information. This process involves several domains in the IMPF.  The team quickly identify that the [Queensland Public Sector Intellectual Property Guidelines](https://www.qld.gov.au/dsiti/assets/documents/ip-principles.pdf) and the Australian Government Intellectual Property Manual provide supporting guidance on recording IP for management and also note the ICT profiling standard may be relevant. They contact the ICT profiling team to access their information asset register to ensure completeness of the IP register. |
| IM-3.4 Information custodianship | Because of the MoG there has been staff movement and some custodianship details require updating. To help make decisions about each IP asset, responsible custodians for each information asset are identified or confirmed. These details are also added to the register.  The custodian of the IP asset will be able to provide information on how the IP was developed; what it is currently used for; if the asset is current and relevant; and if there are constraints to release the asset to the public. |
| IM-5 Record creation and capture | The IP team needs to ensure all IP assets are recorded according to the mandatory principles of the [Records governance policy](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/records-governance-policy). The IP register will need to comply with legal, administrative, cultural and business recordkeeping requirements. |
| IS-4 Asset management | With the custodian of each IP asset the information’s security classification is reviewed or assessed using the [Queensland Government Information Security Classification Framework](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/information-security-classification-framework-qgiscf). This helps the department understand what IP can be released under a Creative Commons license. The security classification is also added to the register. |
| IM-4.2 Licensing and rights management | In the case of the IP assets security classified as PUBLIC the team ensure the IP is licensed using the Creative Commons license. They identify relevant Queensland Government policy and guidance classified to this domain (e.g. [Information access and use policy (IS33),](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/information-access-and-use-policy-is33) [Queensland Public Sector Intellectual Property Guidelines](https://www.qld.gov.au/dsiti/assets/documents/ip-principles.pdf) that encourage the use of the least restrictive Creative Commons license supporting reuse). |
| IM-4.8 Publishing and release | Suitable copyright information (i.e. PUBLIC security classification and Creative Commons license applied) is identified for publication. In the case of open data, the team works with custodians and the open data team to release or update this information on the [Open data portal](https://data.qld.gov.au/). |

### Scenario 3: Open data

Department B has also assessed its open data processes and found a need to boost staff awareness and capability in making decisions about releasing data. The open data team commence scoping an initiative to deliver this. As part of the scoping exercise they review the domains of IMPF to identify areas that staff might need additional support to help with decision making. These include custodianship, information security asset management, privacy, publishing and release and licensing.

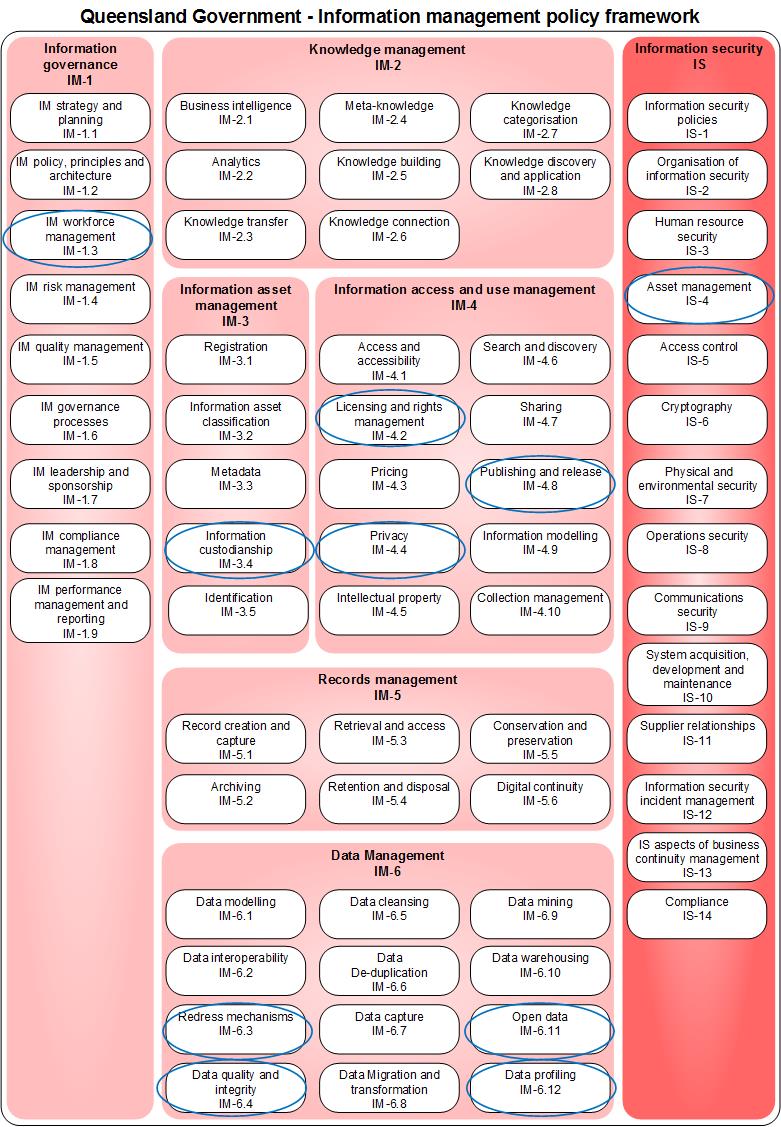


Figure 5 Open data initiative scoping

The table below breaks down the activities that occur in this initiative in each domain. It also demonstrates how relevant support is identified via the IMPF as the department has classified its policies and guidance to the IMPF.

| Domain | Activity |
| --- | --- |
| IM-1.3 IM workforce management | The department has identified a training and development need for open data processes. The IM team work with human resources to develop a strategy for meeting this need. |
| IM-3.4 Information custodianship | Information custodians are responsible for making decisions about the publication and release of their information assets. The team identify resources that can help both explain the roles and responsibilities of custodians and other responsible staff in the context of open data. These were easy for the team to identify as they were classified to the IMPF. The documents include:   * the whole-of-government [Information asset custodianship (IS44)](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/information-asset-custodianship-policy-is44) policy and supporting [Information management roles and responsibilities guideline](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/information-management-roles-and-responsibilities-guideline). * specific departmental documentation on the roles or custodians (e.g. approving publication of datasets) and administrators or contact officers (e.g. preparing data for initial publication and refresh) in open data. |
| IS-4 Asset management | Understanding both the security classification process and classifications themselves assist with determining what data may be released. Only data classified as PUBLIC may be released. As relevant policies have been classified to the IMPF the team locate the [Queensland Government Information Security Classification Framework](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/information-security-classification-framework-qgiscf) and also the department’s own information security classification tool that can assist in developing training material. |
| IM-4.4 Privacy | In addition to security considerations, any privacy impacts must be understood and managed. The team locate the resources of the [Office of the Information Commissioner](https://www.oic.qld.gov.au/) and work with the department’s Privacy officer to develop training material. The department’s approach to de-identifying personal data where applicable is also outlined. |
| IM-4.2 Licensing and rights management | In the case of the data security classified as PUBLIC the team ensure that they are licensed using the least restrictive Creative Commons 4.0 International licence. This helps support the objectives of open data by encouraging reuse. They identify relevant Queensland Government policy and guidance classified to this domain (e.g. [Information access and use policy (IS33),](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/information-access-and-use-policy-is33) [Queensland Public Sector Intellectual Property Guidelines](https://www.qld.gov.au/dsiti/assets/documents/ip-principles.pdf) that encourage the use of the least restrictive license supporting reuse). |
| IM-4.8 Publishing and release | The team utilise the departments existing guidance and extract information from the [data.qld.gov.au publishing standards](https://publications.qld.gov.au/dataset/publishing-standards-data-qld-gov-au) to help staff understand the process for approving the release of data and the standards that open data must adhere to. |
| IM-6.3 Redress mechanisms | The team is careful to include training material about how to engage with end users of open data, including feedback on the data itself provided through the data.qld.gov.au portal. In cases where issues or potential enhancements to datasets are suggested, the department’s internal approach to redressing data issues are explained clearly. |
| IM-6.4 Data quality and integrity | As open data is a constant balance between data quality and cost/time/resource availability, the standards of data quality are considered as part of preparing the training materials, particularly against the [standard disclaimer](https://www.qld.gov.au/legal/disclaimer/) published alongside every open dataset. |
| IM-6.11 Open data | When considering training materials, the starting point is the department’s open data policy. This policy outlines the roles and responsibilities, metadata and data standards, licensing and attribution specific to the delivery of open data, as well as reference to a number of other QGEA and departmental documents that are relevant to Queensland Government’s role as a publisher of open data. |
| IM-6.12 Data profiling | The aspects of data profiling, especially those relevant to the validation and automation of publishing real-time and near-real-time open data are considered as part of the training and align to the existing standards and practices of the department. |

### Collaboration opportunities

As all initiatives are classified to this framework the team can identify if there are any other initiatives that are planned or in progress that are touching on similar areas. In the case above, Department B has two initiatives planned that have similarities:

* IM-3.4 Information custodianship
* IS-4 Asset management
* IM-4.2 Licensing and rights management
* IM-4.8 Publishing and release.

The teams meet to investigate collaboration opportunities and find that there is an opportunity to pilot some new training material as part of the IP register project.

Department A and B share information on their initiatives including domain classifications. This information is presented in a whole of Government ICT Console view and the departments can identify that they are both working on initiatives with similar domains. In this case, Department B can share its mature information security classification processes with Department A, saving Department A time.

## Queensland Government IM policy classification

This section classifies a selection of key existing Queensland Government information management related policies and legislation to the Information management policy framework. Domains coloured:

* blue indicate that whole-of-government policy or legislation exists to support information management practice
* white indicate no whole-of-government policy or legislation to support information management practice.

This section was current as at July 2017.

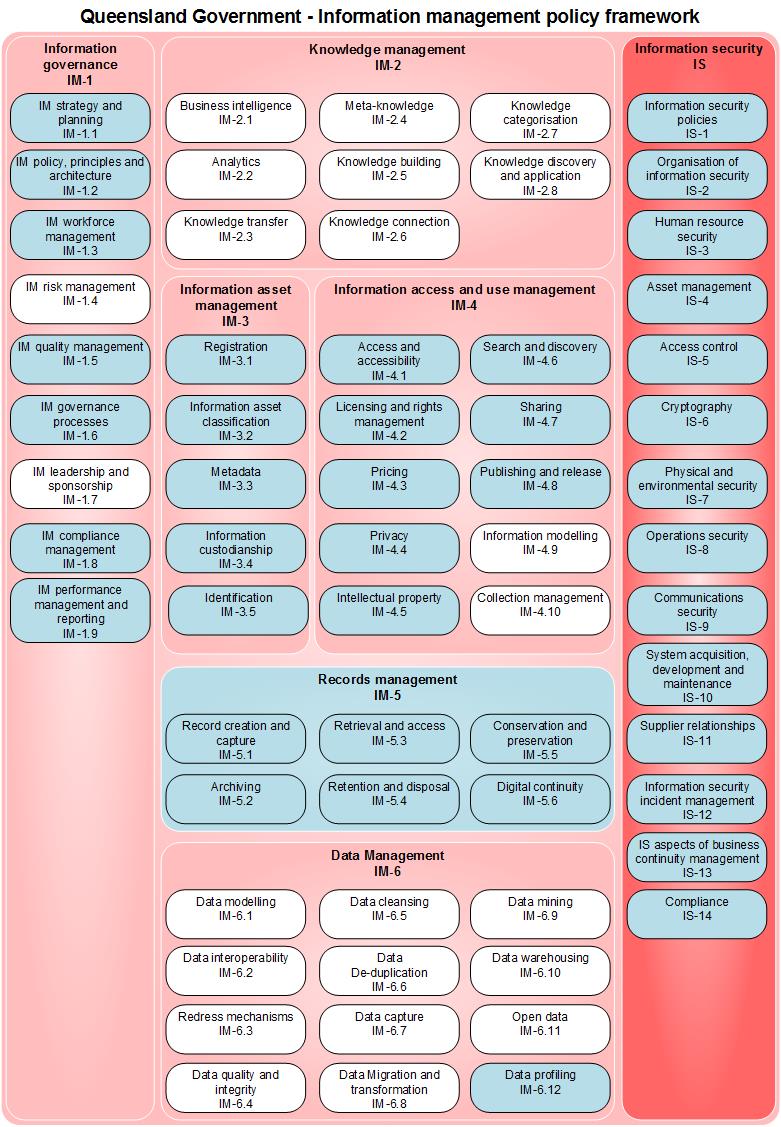


Figure 6 Classification of Queensland Government policies and legislation to framework with blue indicating policy or legislation exists.

The table below provides details of the policies and guidelines classified to each domain.

| ID | Domain | Policy | Notes |
| --- | --- | --- | --- |
| IM-1.1 | IM strategy and planning | ICT resources strategic planning policy (IS2) | Policy requirement 1 |
| IM-1.2 | IM policy, principles and architecture | Information asset custodianship policy (IS44) | Policy requirement 2 |
| IM-1.3 | IM workforce management | Information asset custodianship policy (IS44) | Policy requirement 2 |
| Information standard 40: Recordkeeping (IS40) | Principle 3, 4 |
| IM-1.5 | IM quality management processes | Information standard 34: Metadata (IS34) | Principle 2 |
| Websites policy (IS26) | Policy requirement 2 |
| IM-1.6 | Information governance processes | Information governance policy | Policy requirement 1 |
| Websites policy (IS26) | Policy requirement 2 |
| IM-1.8 | Compliance management | Information standard 40: Recordkeeping (IS40) | Principle 2 |
| IM-1.9 | IM performance management and reporting | ICT resources strategic planning policy (IS2) | Reporting requirements |
| IM-3.1 | Registration | Information asset custodianship policy (IS44) | Policy requirement 1 |
| IM-3.2 | Information asset classification | ICT resources strategic planning policy (IS2) | Policy requirement 1 and Information classification framework |
| IM-3.3 | Metadata | Information standard 34: Metadata (IS34) | Principle 1, 2 and 3 |
| IM-3.4 | Information custodianship | Information asset custodianship policy (IS44) | Policy requirement 2 |
| IM-3.5 | Identification | Information asset custodianship policy (IS44) | Policy requirement 1 |
| IM-4.1 | Access and accessibility | Information access and use policy (IS33) | Policy requirement 1 |
| Websites policy (IS26) | Policy requirement 1 |
| IM-4.2 | Licensing and rights management | Information access and use policy (IS33) | Policy requirement 4 |
| Intellectual property principles (Qld) |  |
| IM-4.3 | Pricing | Information access and use policy (IS33) | Policy requirement 3 |
| IM-4.4 | Privacy | Information Privacy Act 2009 (Qld) |  |
| IM-4.5 | Intellectual property | Intellectual property principles (Qld) |  |
| IM-4.6 | Search and discover | Metadata (IS34) | Principle 3 |
| IM-4.7 | Sharing | Information access and use policy (IS33) | Policy requirement 2 |
| IM-4.8 | Publishing and release | Websites policy (IS26) | Policy requirement 1 |
| IM-5 | Records management | Information standard 40: Recordkeeping (IS40) | Principle 1, 2, 3, 4, 6 |
| Recordkeeping act 2002 (Qld) |  |
| IM-5.1 | Record creation and capture | Information standard 40: Recordkeeping (IS40) | Principle 1 |
| IM-5.2 | Archiving | Recordkeeping act 2002 (Qld) |  |
| Information standard 31: Retention and disposal of records (IS31) | Principle 2 |
| IM-5.3 | Retrieval and access | Information standard 40: Recordkeeping (IS40) | Principle 5 |
| IM-5.4 | Retention and disposal | Information standard 40: Recordkeeping (IS40) | Principle 7 |
| Information standard 31: Retention and disposal of records (IS31) | Principle 1 |
| IM-5.5 | Conservation and preservation | Information standard 40: Recordkeeping (IS40) | Principle 7 |
| IM-5.6 | Digital continuity | Information standard 40: Recordkeeping (IS40) | Principle 7 |
| IM-6.12 | Data profiling | ICT resources strategic planning policy (IS2) | Reporting requirements |
| IS-1 | Information security policies | Information standard 18: Information security (IS18) | Principle 1 |
| IS-2 | Organisation of information security | Information standard 18: Information security (IS18) | Principle 7 |
| IS-3 | Human resource security | Information standard 18: Information security (IS18) | Principle 3 |
| IS-4 | Asset management | Information standard 18: Information security (IS18) | Principle 2, 5 |
| IS-5 | Access control | Information standard 18: Information security (IS18) | Principle 6 |
| Information standard 40: Recordkeeping (IS40) | Principle 5 |
| IS-6 | Cryptography | Information standard 18: Information security (IS18) | Principle 5 |
| IS-7 | Physical and environmental management | Information standard 18: Information security (IS18) | Principle 4 |
| IS-8 | Operations security | Information standard 18: Information security (IS18) | Principle 5, 6, 7 |
| IS-9 | Communications security | Information standard 18: Information security (IS18) | Principle 5, 6 |
| IS-10 | System, acquisition, development and maintenance | Information standard 18: Information security (IS18) | Principle 5, 7 |
| IS-11 | Supplier relationships | Information standard 18: Information security (IS18) | Principle 1, 5, 9 |
| IS-12 | Information security incident management | Information standard 18: Information security (IS18) | Principle 8 |
| IS-13 | IS aspects of business continuity management | Information standard 18: Information security (IS18) | Principle 9 |
| IS-14 | Compliance management | Information standard 18: Information security (IS18) | Principle 7, 10 |

Summary of changes

This section summarises changes from the previous version of the Information management policy framework. The diagram below provides a visual representation of changes in the new framework which are explained further in sections A.1, A.2, A.3. Section A.4 highlights deleted domains from the previous version of this framework.

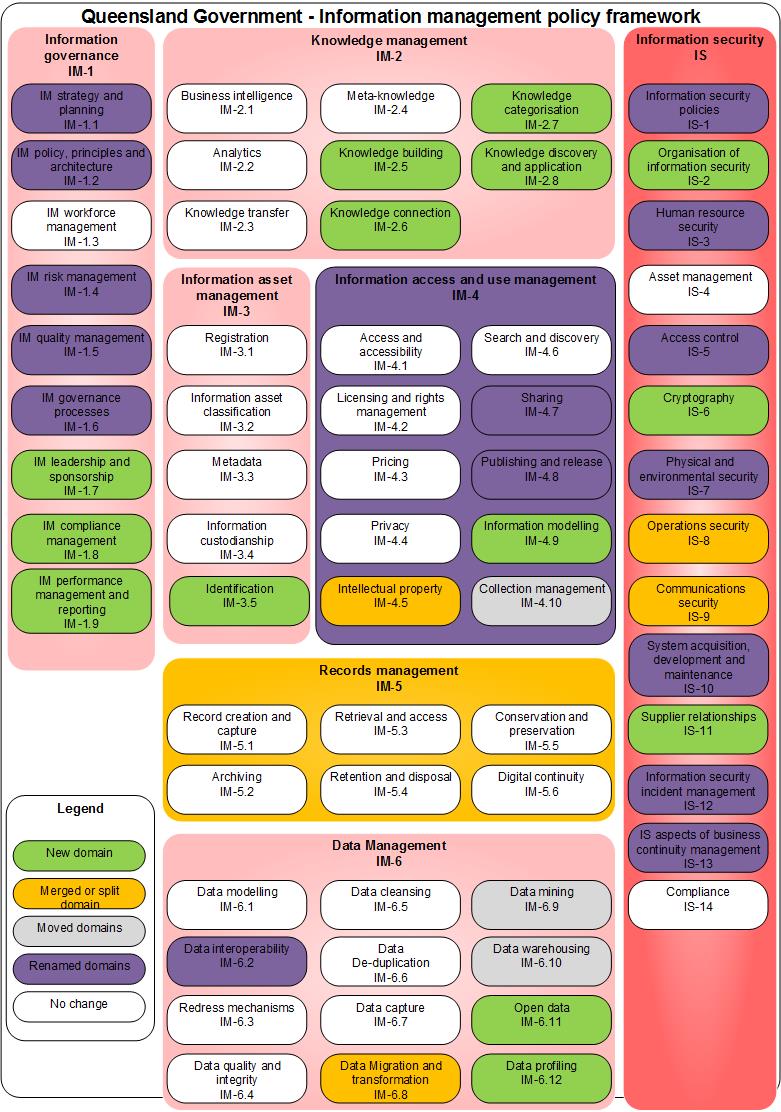


Figure 7 Summary of changes to Information management policy framework

New, merged and split domains

|  |  |
| --- | --- |
| Current framework domain | Notes |
| IM-1.7 IM leadership and sponsorship | New domain |
| IM-1.8 IM compliance management | New domain |
| IM-1.9 IM performance management and reporting | New domain and includes former Reporting domain |
| IM-2.5 Knowledge building | New domain |
| IM-2.6 Knowledge connection | New domain |
| IM-2.7 Knowledge categorisation | New domain |
| IM-2.8 Knowledge discovery and application | New domain |
| IM-3.5 Identification | New domain |
| IM-4.5 Intellectual property | Merged domain. Now includes IM-4.6 Copyright. |
| IM-4.9 Information modelling | New domain |
| IM-5 Records management | Merged domain.  Merge between IM-5 Recordkeeping and IM-5.1 Record management in previous framework. |
| IM-6.8 Data migration and transformation | Merged domain. Previously IM-6.8 Data migration and IM-6.9 Data conversion and transformation. |
| IM-6.11 Open data | New domain |
| IM-6.14 Data profiling | New domain |
| IS-2 Organisation of information security | New domain |
| IS-6 Cryptography | New domain |
| IS-8 Operations security | Split domain. Previously part of IS-5 Communications and operations management. |
| IS-9 Communications security | Split domain. Previously part of IS-5 Communications and operations management. |
| IS-11 Supplier relationship | New domain |

Renamed domains

| Current framework domain | Notes |
| --- | --- |
| IM-1.1 IM strategy and planning | Previously IM-1.1 Information and IM strategy and planning |
| IM-1.2 IM policy, principles and architecture | Previously IM-1.2 Information and IM policy, principles and architecture |
| IM-1.4 IM risk management | Previously IM-1.4 Information and IM risk management |
| IM-1.5 IM quality management | Previously IM-1.5 Information and IM quality management |
| IM-1.6 Information governance processes | Previously IM-1.6 Information governance processes |
| IM-4 Information access and use management | Previously IM-4 Information asset access and use management |
| IM-4.8 Publishing and release | Previously IM-4.9 Publishing |
| IM-6.2 Data interoperability | Previously IM-6.2 Data integration |
| IS-1 Information security policies | Previously IS-1 Policy, planning and governance |
| IS-3 Human resources security | Previously IS-3 Human resources management |
| IS-7 Physical and environmental security | Previously IS-4 Physical and environmental management |
| IS-5 Access control | Previously IS-6 Access management |
| IS-10 System acquisition, development and maintenance | Previously IS-7 System acquisition, development and management |
| IS-12 Information security incident management | Previously IS-8 Incident management |
| IS-13 Information security aspects of business continuity management | Previously IS-9 Business continuity management |

Moved domains

|  |  |
| --- | --- |
| Current framework domain | Notes |
| IM-2.6 Reporting | Moved to new domain IM-1.9 IM performance and reporting. |
| IM-4.10 Collection management | Previously located in IM-5 Records management and known as IM-5.3 Collection management. |
| IM-6.9 Data mining | Previously located in IM-2 Knowledge management and known as IM-6.2 Data mining. |
| IM-6.10 Data warehousing | Moved from IM-2 Knowledge management previously known as IM-2.4 Data warehousing. |

Deleted domains

The following domains were in the previous version of the framework and have now been deleted or merged:

| Previous framework domain | Notes |
| --- | --- |
| IM-4.6 Copyright | Merged. See IM-4.5 Intellectual property in revised framework. |
| IM-5.1 Record management | Merged and renamed. See IM-5 Records management in revised framework. |
| IM-6.8 Data migration | Merged. See IM-6.8 Data migration and transformation in revised framework. |
| IM-6.9 Data conversion and transformation | Merged. See IM-6.8 Data migration and transformation in revised framework. |
| IS-5 Communications and operations management | This has been split. See IS-8 Operations security and IS-9 Communications security in revised framework. |

1. Queensland Government Chief Information Office, *Glossary*, available at https://www.qgcio.qld.gov.au/products/glossary, accessed 7 June 2017. [↑](#footnote-ref-2)
2. Standards Australia, *AS 5037-2005 Knowledge management a guide,* 2005. [↑](#footnote-ref-3)
3. Australian Quality Council, *Australian business excellence framework,* 2002. [↑](#footnote-ref-4)
4. Queensland State Archives, *Glossary of Archival and Recordkeeping Terms,* available at <https://www.forgov.qld.gov.au/glossary?keys=records&=Search>, accessed 4 May 2017. [↑](#footnote-ref-5)
5. Standards Australia, *AS ISO/IEC 38500:2016 Corporate Governance of Information Technology,* 2016, p. 2. [↑](#footnote-ref-6)
6. Queensland Government Chief Information Office, *Best Practice Guide: Information Risk Management,* 2002, p. 4-5. [↑](#footnote-ref-7)
7. Standards Australia, *AS/NZS ISO 9000: 2016 Quality management systems – Fundamentals and vocabulary,* 2016, p. 14. [↑](#footnote-ref-8)
8. Glossary’, *gotcha!,* available at <http://www2.sims.berkeley.edu/courses/is213/s99/Projects/P9/web_site/glossary.htm#K>, accessed 4 May 2017 [↑](#footnote-ref-9)
9. Knowledge building’, *Wikipedia,* available at <https://en.wikipedia.org/wiki/Knowledge_building>, accessed 16 January 2017. [↑](#footnote-ref-10)
10. MIT Press, “Introduction to Knowledge Management”, Ch. 1, pg. 22, available at <https://mitpress.mit.edu/sites/default/files/titles/content/9780262015080_sch_0001.pdf>, accessed 16 January 2017. [↑](#footnote-ref-11)
11. “Categorization”, *Wikipedia*, available at <https://en.wikipedia.org/wiki/Categorization>, accessed 16 January 2017. [↑](#footnote-ref-12)
12. Framework for Information and Knowledge Management”, *Tallin University*, available at <http://www.tlu.ee/~sirvir/Information%20and%20Knowledge%20Management/Framework%20for%20IKM/knowledge_management_processes_knowledge_application.html>, accessed 27 February, 2017. [↑](#footnote-ref-13)
13. Bailey, S. ‘Do you need a taxonomy strategy?’, *Inside Knowledge,* vol. 5, no. 5, 2002, available at <http://www.kmmagazine.com/xq/asp/sid.9A5D0B8D-6922-11D7-9D48-00508B44AB3A/articleid.E4F31EEC-FB65-413A-A24B-13AA6ACDD12D/qx/display.htm>, accessed 19 March 2009 [↑](#footnote-ref-14)
14. Queensland Government Chief Information Office, *Glossary – M,* available at <http://www.qgcio.qld.gov.au/qgcio/resources/glossary/Pages/glossarym.aspx>, accessed 19 March 2009. [↑](#footnote-ref-15)
15. ‘The data spectrum’, *ODI: Open data institute,* available at <https://theodi.org/data-spectrum>, accessed 4 May 2017, used under the Creative Commons Attribution-ShareAlike 2.0 UK: England & Wales (CCBY-SA 2.0 UK). To view a copy of this licence, visit <https://creativecommons.org/licenses/by-sa/2.0/uk/deed.en_GB> [↑](#footnote-ref-16)
16. ‘Information rights management’, *Wikipedia,* available at <https://en.wikipedia.org/wiki/Information_rights_management>, accessed 4 May 2017. [↑](#footnote-ref-17)
17. Queensland Government, *Queensland Public Sector Intellectual Property Principles,* 2013, p. 4. Available at <https://www.forgov.qld.gov.au/__data/assets/pdf_file/0024/182706/qps-ip-principlesfinal-v.2.pdf>, accessed 4 May 2017, used under the Creative Commons Attribution Non-Commercial No Derivatives (BY-NC-ND) 3.0 licence Australia. To view a copy of this licence, visit <https://creativecommons.org/licenses/by-nc-nd/3.0/au/deed.en> [↑](#footnote-ref-18)
18. Treasury Board of Canada, *Glossary – Subject: Resource Discovery*, available at <http://www.tbs-sct.gc.ca/cioscripts/gloss/gloss-alpha_e.asp?SubjectID=134&who=/im-gi/>, accessed 19 March 2009. [↑](#footnote-ref-19)
19. Office of Information Commissioner Queensland, Administrative release of information, available at <https://www.oic.qld.gov.au/guidelines/for-government/access-and-amendment/proactive-disclosure/administrative-release-of-information>, accessed 9 January 2017, used under the Creative Commons Attribution 4.0 (CC-BY) licence. To view a copy of this licence visit <https://creativecommons.org/licenses/by/4.0/> [↑](#footnote-ref-20)
20. Department of Education and Training, *Information Management Strategic Framework v1.2*. [↑](#footnote-ref-21)
21. ISO 15489-1:2016 Information and documentation – Records management – Part 1: Concept and principles. [↑](#footnote-ref-22)
22. Queensland State Archives, *Glossary,* available at <https://www.forgov.qld.gov.au/glossary>, accessed 1 June 2017. [↑](#footnote-ref-23)
23. Ibid. [↑](#footnote-ref-24)
24. Ibid. [↑](#footnote-ref-25)
25. Ibid. [↑](#footnote-ref-26)
26. Ibid. [↑](#footnote-ref-27)
27. Ibid. [↑](#footnote-ref-28)
28. ‘Data modeling’, *Wikipedia*, available at <http://en.wikipedia.org/wiki/Data_modeling>, accessed10 May 2017. [↑](#footnote-ref-29)
29. ‘Data Interoperability’, *Defined Term*, available at <https://definedterm.com/data_interoperability>, accessed 9 January 2017. [↑](#footnote-ref-30)
30. ‘Data integration’, *Wikipedia,* available at <http://en.wikipedia.org/wiki/Data_integration#cite_note-refone-0>, accessed 19 March 2009. [↑](#footnote-ref-31)
31. Office of Economic Co-operation and Development, *OECD Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information,* 2008, p. 5. Available at [www.oecd.org/dataoecd/0/27/40826024.pdf](http://www.oecd.org/dataoecd/0/27/40826024.pdf), accessed 17 May 2017. [↑](#footnote-ref-32)
32. Ibid, p. 6. [↑](#footnote-ref-33)
33. ‘Data cleansing’, *Wikipedia*, available at <http://en.wikipedia.org/wiki/Data_cleansing>, accessed 17 May 2017. [↑](#footnote-ref-34)
34. ‘Data deduplication’, *Wikipedia,* available at <http://en.wikipedia.org/wiki/Data_deduplication>, accessed 17 May 2017. [↑](#footnote-ref-35)
35. ‘Data migration’, *Wikipedia*, available at <http://en.wikipedia.org/wiki/Data_migration>, accessed 17 May 2017. [↑](#footnote-ref-36)
36. ‘Data transformation’, *Wikipedia*, available at <http://en.wikipedia.org/wiki/Data_transformation>, accessed 17 May 2017. [↑](#footnote-ref-37)
37. “Data Mining: What is Data Mining”, *UCLA*, available at <http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm>, accessed 16 January 2017. [↑](#footnote-ref-38)
38. Data warehouse”, *Wikipedia,* available at <https://en.wikipedia.org/wiki/Data_warehouse>, access 16 January 2017. [↑](#footnote-ref-39)
39. ‘What is open data?’, *Open Data Institute,* available at <https://theodi.org/what-is-open-data>, accessed 9 January 2017, used under the Creative Commons Attribution-ShareAlike 2.0 UK: England & Wales (CCBY-SA 2.0 UK). To view a copy of this licence, visit <https://creativecommons.org/licenses/by-sa/2.0/uk/deed.en_GB> [↑](#footnote-ref-40)
40. ‘Data profiling’, *Wikipedia,* available at <https://en.wikipedia.org/wiki/Data_profiling>, accessed 9 January 2017. [↑](#footnote-ref-41)