



HM Government

Government Functional Standard

GovS 005: Digital

Version: 2.2

Date issued: September 2026



Government Functional Standard

This functional standard is part of a suite of management standards that promotes consistent and coherent ways of working across government, and provides a stable basis for assurance, risk management and capability improvement.

The suite of standards, and associated guidance, can be found at **GOV.UK government functional standards**.

Functional standards cross-refer to each other where needed, so can be confidently used together.

They contain both mandatory and advisory elements, described in consistent language (see the table below).

Term	Intention
shall	denotes a requirement: a mandatory element.
should	denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	denotes a description.

The meaning of words is as defined in the Shorter Oxford English Dictionary, except where defined in the Glossary in **Annex B**.

It is assumed that legal and regulatory requirements are always met.

Version 2.2 of GovS005 replaces version 2.1. Minor update, Version 2.2 updates the standard from a digital, data and technology focus to a broader government digital and data standard, simplifies and modernises much of the language, and strengthens lifecycle management, governance and accountability throughout. It also introduces extensive new content on the safe, secure, transparent and responsible use of artificial intelligence (AI), embedding AI considerations across governance, strategy, assurance, service management, technology, data and risk management.

© Crown copyright 2026

Produced by the Government Digital and Data function

You may re-use this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, visit:

www.nationalarchives.gov.uk/doc/open-government-licence/ or email:
psi@nationalarchives.gsi.gov.uk

Where we have identified any third-party copyright material you will need to obtain permission from the copyright holders concerned.

Contents

Contents	3
1. Purpose and Scope	6
1.1 Purpose of this standard	6
1.2 Scope of this standard	6
1.3 Government standards references	6
2. Principles	7
3. Context	7
3.1 Introduction	7
3.2 Digital transformation	8
3.3 Services	8
3.4 Technology	8
3.5 Data	8
4. Governance	9
4.1 Governance and management framework	9
4.2 Strategy and planning	10
4.3 Assurance	11
4.4 Decision making	12
4.5 Risk management	13
4.6 Roles and accountabilities	13
5. Service management	17
5.1 Overview	17
5.2 Policy intent	17
5.3 Service design and development	18
5.4 Service management	18
5.5 Management of the organisation's portfolio of services	19
5.6 Performance metrics and feedback	19
5.7 Accessible and inclusive services	19
5.8 Service retirement	20
6. Technology management	20
6.1 Overview	20
6.2 Technology development and maintenance	21
6.3 Deployment and operation of technology	21
6.4 Retirement of government digital and data solutions	22
7. Data management	24
7.1 Overview	24
7.2 Data management principles	25



Government Functional Standard

7.3 Data frameworks and operating models	26
7.4 Data architecture	26
7.5 Data and information asset management.....	27
7.6 Data engineering	28
8. Digital management practices.....	29
8.1 Overview	29
8.2 Delivery approach.....	29
8.3 User-centred design	30
8.4 System integration and interoperability.....	31
8.5 Knowledge and information management	31
8.6 Use of channels and user engagement	31
8.7 Sustainability.....	32
8.8 Configuration and asset management.....	32
8.9 Performance management.....	33
8.10 Management information, analytics and reporting	33
18.12 Purchasing and contract management.....	34
A. References	35
B. Glossary	36

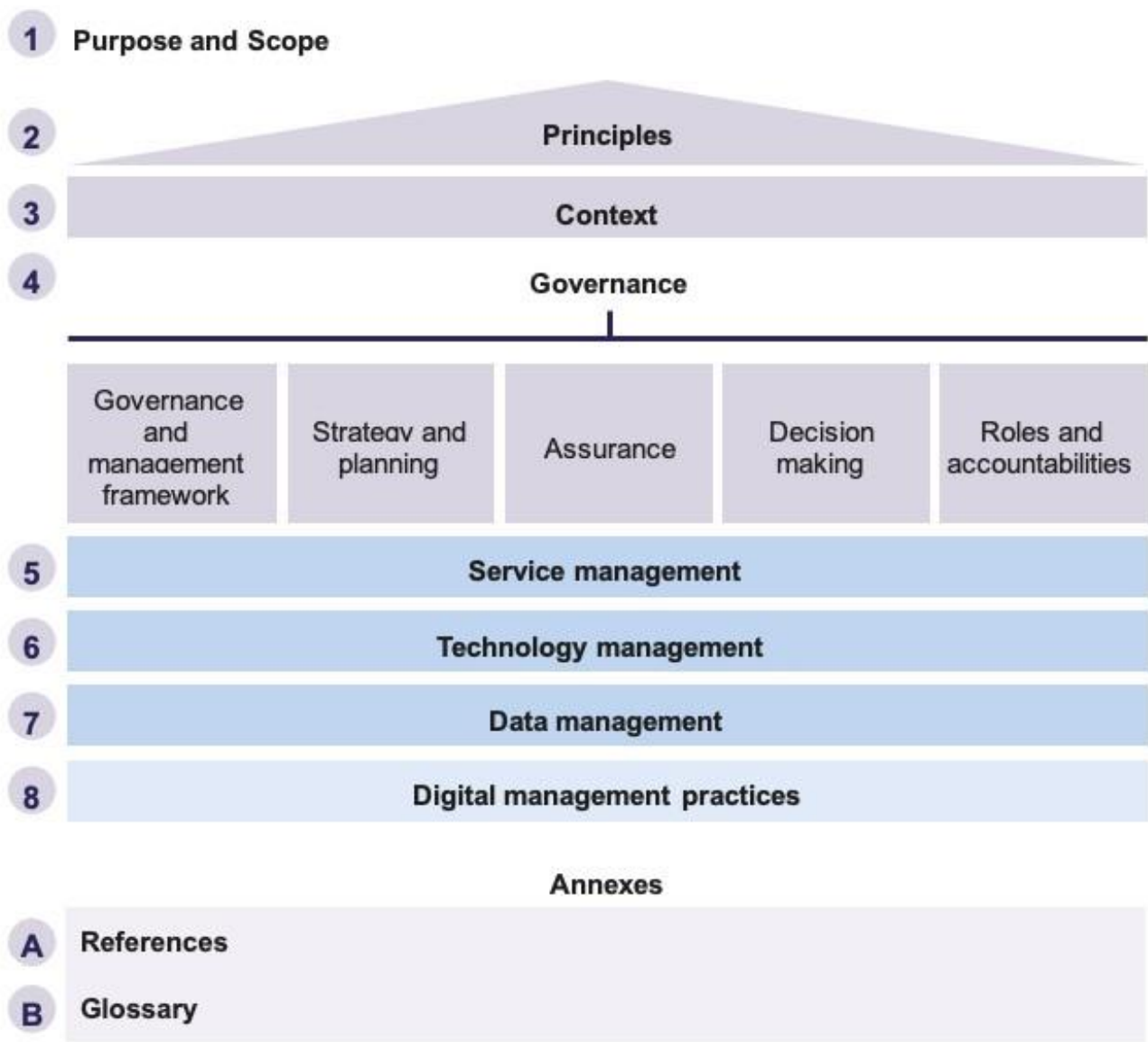


Figure 1 Structure and scope of this standard



1. Purpose and Scope

1.1 Purpose of this standard

This standard sets out what government organisations shall do to govern, deliver and assure digital and data activity. It helps organisations improve public services, work more efficiently and manage risk.

Organisations shall use a consistent approach so digital and data activity:

- supports agreed policy and mission outcomes
- makes public services easier to access, use and improve
- improves productivity and efficiency across government
- supports services and platforms that work together, can scale and is resilient
- uses data to make decisions and improve continuously

This standard is for:

- senior accountable leaders, including permanent secretaries, directors general and chief executives of arm's length bodies
- senior leaders accountable for digital and data, including chief digital and information officers and chief data officers
- senior leaders responsible for strategy, policy or service delivery
- practitioners who plan, deliver, operate or manage digital and data activity

1.2 Scope of this standard

This standard applies to the whole lifecycle of government digital and data activity. This includes planning, designing, delivering, running and retiring:

- public-facing and internal services
- technology and platforms
- data and data products

This standard shall apply to government departments, arm's length bodies and any other organisation in scope of a government functional standard.

GovS 005 addresses the governance, delivery, operation, resilience and lifecycle management of digital services, data and technology.

Cyber security requirements, controls and assurance expectations are set through GovS 007: Security.

Organisations should apply both standards together to ensure digital resilience and cyber security are managed coherently.

Other public sector organisations, including devolved administrations and local government, may adopt this standard or use it to support benchmarking and improvement.

1.3 Government standards references

Organisations should use this standard with other relevant government functional standards set out on GOV.UK. Each standard should be applied according to its own scope and accountabilities. [1]

This standard is supported by The Service Standard [2], which sets expectations for services, and the Technology Code of Practice [3], which sets expectations for technology decisions.

The following standards are directly necessary for the use of this standard:

- GovS 002, Project delivery
- GovS 003, Human resources
- GovS 006, Finance
- GovS 007, Security
- GovS 008, Commercial
- GovS 009, Internal audit
- GovS 010, Analysis
- GovS 013, Counter fraud

Together, these standards explain how government digital and data activity shall be governed, delivered, secured, measured and assured.

2. Principles

These principles set the expectations for how government digital and data activity should be planned, governed, delivered and improved to achieve user-centred, secure and measurable public outcomes.

They should provide clarity between organisational objectives, accountable delivery, proportionate assurance and continuous improvement across the full service and product lifecycle.

To strengthen their impact, the principles should be applied as strategic expectations, supported by evidence of ownership, risk management, performance, interoperability, data governance and ethical practice.

Anyone responsible for planning, developing, delivering or managing government digital and data activity shall ensure:

1. digital and data activity is aligned with government priorities, organisational

objectives and the outcomes needed by users and the public

2. governance, assurance and decision making are proportionate to the scale, stage and risk of the work
3. accountability, ownership and responsibilities are clear across organisational and delivery boundaries
4. services and products are designed around evidenced user needs, accessibility, inclusion and measurable outcomes
5. services, products and technology are managed throughout their lifecycle using evidence, feedback and performance data
6. technology and data are managed securely, lawfully and ethically, with appropriate controls for resilience, interoperability and reuse
7. teams have the skills, capacity and authority needed to deliver effectively and uphold public service values and professional standards
8. options and decisions are informed by a proportionate analysis of uncertainty, including risks, opportunities, assumptions and dependencies, taking into account the chances of different degrees of success or failure
9. government digital and data activity delivers value for money, in alignment with Managing Public Money, securing the appropriate combination of economy, efficiency and effectiveness needed to achieve the intended outcome

3. Context

3.1 Introduction

This section explains the context for applying this functional standard. It sets out



how government digital and data capabilities support policy outcomes, improve services, strengthen assurance, manage risk and help organisations work better.

3.2 Digital transformation

Digital transformation means improving how government designs, delivers and manages services. Services should be simple, accessible, secure and efficient for users and organisations.

This includes improving whole services and processes, using data well, and making sure technology is secure, sustainable, interoperable and aligned to user and policy needs.

Effective delivery needs clear ownership across the lifecycle, multidisciplinary working and continuous improvement across services, technology and data. This means:

- identifying accountable owners for services, products, technology and data across their lifecycle
- using multidisciplinary teams to work across organisational boundaries, improve outcomes, manage risk, measure performance and improve delivery

3.3 Services

A service helps users achieve an outcome. It should reflect policy intent, legal requirements, operational needs and user needs.

Services can be public facing, such as applying for a licence, or internal, such as platforms that support finance, human resources or case management.

A service can include digital and non-digital parts that work together across the whole user journey. Digital parts can include online forms, notifications, application

programming interfaces and casework tools. Non-digital parts can include assisted digital support, post, telephone contact and face-to-face interactions.

3.4 Technology

Technology means the systems, platforms, infrastructure, applications and tools used to deliver, run, secure and improve government services and organisational capabilities.

This includes physical and cloud infrastructure, networks, end-user devices, hosting environments and other components used to create, process, store, secure and share information.

This includes artificial intelligence technologies. Organisations should select, buy, deploy and manage them safely, securely and responsibly, with clear lifecycle ownership, assurance, proportionate risk management and meaningful human control at the right stages.

Technology also includes software, applications, integrations, automation and code used to:

- provide interfaces for users, staff and other systems
- support policy delivery, operational processes, service management and decision making

3.5 Data

Data is information that government collects, creates, uses, shares and manages. It helps government understand needs, make decisions, deliver services, monitor performance, manage risk and improve outcomes.

Where data supports artificial intelligence tools, organisations should make sure it is lawful, relevant, accurate, secure and properly governed. They should identify and

manage risks relating to privacy, fairness, bias, transparency and information quality.

Types of data include:

- personal data, such as names, contact details and identifiers
- location and environmental data, such as geospatial reference data
- administrative and operational data about organisations, assets, services and transactions

Uses for data in government include:

- informing policy design, development, implementation and evaluation
- monitor and report on performance, outcomes, risk and value for money
- support service delivery and improvement, including eligibility checks, case management and service analytics
- help organisations understand performance, manage risk and make evidence-based decisions

Organisations applying this standard should treat services, technology and data as connected parts of one delivery system. They should build clear ownership, proportionate assurance and continuous improvement into how they plan, deliver and manage outcomes.

4. Governance

4.1 Governance and management framework

4.1.1 Overview

Governance covers prioritising, authorising, empowering, overseeing and assuring

performance across government and within each organisation.

A governance and management framework shall be defined by those accountable for government digital and data activity. It should ensure governance is effective, proportionate, structured and aligned with cross-government priorities, including the safe, secure and responsible use of artificial intelligence.

It should include:

- delegated authority limits, decision making roles and rules, assurance needs, reporting structures, accountabilities and escalation routes
- management practices and documentation needed to meet this standard, including records of significant digital, data and AI-enabled systems where appropriate
- risk appetite and tolerance, risk ownership, reporting, oversight and escalation arrangements within the governance and management framework

4.1.2 Governance across government

A senior officer accountable for government digital and data strategy and planning across government shall be assigned (see 4.6.2). They should define the cross-government governance and management framework in consultation with organisational digital and data leaders (see 4.6.4).

The cross-government governance and management framework should include:

- arrangements for developing and monitoring cross-government digital strategies and plans (see 4.2.1)
- cross-government service, technology and data standards



Government Functional Standard

- capability requirements
 - guidance for practitioners
 - expectations for responsible AI adoption
 - arrangements for identifying, assessing and managing systemic digital, data and technology risks
 - a pipeline of proposed, current and completed work, including associated spend
- A senior officer accountable for the governance of the organisation's government digital and data portfolio shall be assigned (see 4.6.4).

4.1.3 Governance within each organisation

Governance of government digital and data work within an organisation should be integrated with the organisation's overall governance. The framework should bring together digital, data, service, technology, AI and wider business leaders so that work is prioritised, funded, delivered and improved in line with organisational objectives.

Each organisation's governance and management framework should comply with:

- government and departmental policies
- this functional standard and other relevant functional standards (see 1.2)
- cross-government standards and requirements (see 4.1.2)
- applicable AI guidance, ethics requirements, data protection obligations, security standards and assurance expectations
- statutory requirements

As part of the governance and management framework, each organisation should develop and maintain:

- required strategies and plans (see 4.2)

4.2 Strategy and planning

4.2.1 Cross-government digital strategy

A cross-government strategy shall be developed and maintained to set the ambition for modern digital government and guide government digital and data work in organisations. It should reach at least three to five years into the future and set expectations for:

- synergy, efficiency and interoperability of government digital and data activity, services, technology, data and related assets within and among organisations
- identifying and managing principal and systemic digital, data and technology risks, opportunities and dependencies across government
- significant programmes
- how organisational and government digital and data outcomes and targets will be achieved
- capability and capacity requirements
- how the strategy is to be implemented
- how AI and automation will be adopted responsibly to improve public services, productivity and decision support while maintaining public trust

The cross-government digital and data strategy shall be developed in collaboration with senior business leaders and

government digital and data specialists across government. It shall be communicated to organisations and used to support decision making (see 4.4).

Note: For current cross-government digital, data and AI expectations, see relevant government digital and data strategy, policy and guidance. [4]

Note: For data and information, see the National Data Library. [5]

4.2.2 Digital strategy and planning in an organisation

Each organisation should define and implement a government digital and data strategy, which shall:

- align to the cross-government digital and data strategy (see 4.2.1)
- align to the organisation's policy and strategy
- be subject to approval by the accounting officer (see 4.6.3)
- set out how AI will be used safely, lawfully, ethically and effectively, where relevant to organisational objectives

The government digital and data strategy should be developed collaboratively by the organisation's senior leaders and led by the senior officer accountable for the organisation's government digital and data portfolio (see 4.6.4). It should reach at least three to five years into the future, and should:

- outline the organisation's ambition for how government digital and data capabilities will be used to achieve the organisation's objectives
- include benchmarks which enable assessment of the organisation's

current performance and effectiveness

- outline plans for how the organisation will achieve its objectives for digital services, data, technology and capability
- describe the data, skills, governance and assurance needed to support responsible AI adoption

The government digital and data strategy should be endorsed and actively supported by the accounting officer (see 4.6.3) and senior leadership, as this is critical to achieving effective digital transformation and better outcomes.

A detailed plan for government digital and data activity should set out owners, milestones, dependencies, risks and key performance indicators. Where AI is used, the plan should also define the intended benefits, data requirements, human oversight, assurance approach, model or tool ownership, monitoring arrangements and route for escalating risks. Plans should be agreed with relevant senior leaders and reviewed through governance and performance reporting.

4.3 Assurance

Assurance provides confidence to senior leaders and stakeholders that work is controlled, proportionate and supports successful delivery of policy, strategy and objectives.

Organisations should have a defined approach to assurance of government digital and data spend and activity. Assurance should be proportionate to risk, value and impact, integrated with the organisation's overall assurance framework, and aligned to cross-government strategy, standards and expenditure controls.

AI-enabled activity should be assured across its lifecycle, including use case



selection, data quality, privacy, security, ethical risk, bias, transparency, human oversight, procurement, operational monitoring and retirement. Assurance should confirm that AI is used only where it is appropriate, lawful, secure and supported by the right skills and controls.

Typically, assurance should be on at least three separate and defined levels, including:

- by, or on behalf of, the operational management team that owns and manages risk
- by, or on behalf of, senior management, independent of operational management, using specialist expertise to oversee management of the risk, and to ensure the first line of defence is properly designed and operating as intended
- by independent bodies to provide senior management with an objective opinion on the effectiveness of governance, risk management and internal controls, including the effectiveness of the previous lines of defence

Recommendations provided through assurance processes should be incorporated into delivery planning at the earliest opportunity.

Government Functional Standard GovS 009: Internal Audit shall be complied with. [7]

The requirements of the Orange Book: Management of Risk, Principles and Concepts, including Part II, the Risk Control Framework and its assurance expectations, shall be met. [8]

4.4 Decision making

Decisions relating to government digital and data activity should be made, approved and authorised in a timely way in accordance

with the organisation's governance and management framework. Where specified, minimum expectations shall be met (see 4.2.1).

Options and decisions should be based on clear criteria, evidence and user needs, and informed by a proportionate analysis of benefits and uncertainty, including risks, opportunities, assumptions and dependencies, taking into account the chances of different degrees of success or failure.

Key decisions relating to government digital and data activity should include:

- alignment to cross-government and organisational strategy and plans
- authorising programmes and projects (see Government Functional Standard GovS 002: Project Delivery)
- efficiency and value
- sustainability of options, including the purchase of products and services (see Government Functional Standard GovS 008: Commercial)
- value for money, in alignment with Managing Public Money
- responsible use of AI, including lawfulness, ethics, data protection, transparency, explainability, human oversight, security, model performance and ongoing monitoring

No organisation should make decisions which impact other organisations without having consulted them.

Government Functional Standard GovS 002: Project Delivery shall be complied with, with respect to portfolio, programme or project related decisions (such as initiating a project, authorising a new project phase, or responding to issues and risks).

Government Functional Standard GovS 008: Commercial shall be complied with, with respect to commercial decisions (such as deciding on a third-party supplier).

Government Functional Standard GovS 010: Analysis shall be complied with, with respect to the assessment of options.

Organisations shall comply with expenditure controls guidance. [9]

Organisations shall comply with guidance on how to handle public funds. [10]

4.5 Risk management

Risk management supports informed decision making and helps digital products, services, data and technology operate successfully in support of objectives. It should address uncertainty, threats and opportunities, taking into account the chances of different degrees of success or failure. This includes risks arising from data, cyber security, legacy technology, third parties and AI.

The senior officer accountable for the organisation's digital portfolio (see 4.6.4) should ensure that management of risk is:

- integrated with the organisation's overall risk management strategy
- within the organisation's risk appetite and tolerance
- proportionate to the scale and complexity of the work

Risks associated with government digital and data activity should be represented at board level and reviewed regularly, including risks relating to sustainability of investment, continual improvement, capability, security, legacy technology, technical debt, data quality and AI use.

Digital resilience risks shall be owned, monitored and reported through organisational governance arrangements.

Organisational contingency and business continuity planning should be defined for services where failure presents a clear risk to organisational objectives. Accountability for enacting disaster recovery plans should be defined.

The requirements of the Orange Book: management of risk - principles and concepts, shall be met. [3]

4.6 Roles and accountabilities

4.6.1 Overview

Roles and accountabilities shall be defined in governance and management frameworks and assigned to people with appropriate seniority, skills and experience.

This should include the activities, outputs or outcomes each role is responsible for, who they are accountable to, and how responsibilities are discharged for AI-enabled systems where relevant.

4.6.2 Senior officer accountable for digital strategy and planning across government

The senior officer accountable for government digital and data strategy and planning across government is accountable for:

- providing leadership and direction for government digital and data transformation and policy across government (see 3.2)
- collaborating within the organisation to identify, assess and manage systemic digital, data and technology risks, and supporting collective action to address common vulnerabilities, dependencies and capability gaps



Government Functional Standard

- setting and maintaining the cross-government governance and management framework (see 4.1)
- defining, communicating and implementing the cross-government digital and data strategy, policy and plans (see 4.2.1)
- continuous improvement in the government's use of digital services, technology and data to support improved outcomes (see sections 5, 6, 7 and digital practices in section 8)
- setting expectations for responsible AI adoption across government, including governance, assurance, transparency, capability and risk management

Note: The Government Digital Service, part of the Department for Digital, Culture, Media and Sport, leads the Government Digital and Data function for government.

4.6.3 Accounting officer

The permanent head of a government department is usually its principal accounting officer.

An organisation's accounting officer is accountable (via a principal accounting officer where appropriate) to parliament and the public for the stewardship of public resources, ensuring they are used effectively and to high standards of probity. The principal accounting officer generally appoints the most senior executive in the arm's length bodies within the department's ambit as an accounting officer.

The accounting officer is accountable for ensuring the organisation's government digital and data strategy is appropriate (see 4.2.2), and should create an environment in which their organisation:

- endorses and actively supports government digital and data

transformation

- plans and manages government digital and data activity in accordance with this standard
- uses AI responsibly and proportionately, with appropriate governance, assurance, transparency and human oversight

4.6.4 Senior officer accountable for an organisation's digital portfolio

The senior officer accountable for an organisation's government digital and data portfolio is accountable to the accounting officer for:

- providing leadership and direction for government digital and data transformation within the organisation
- ensuring government and organisational policies are complied with
- setting and maintaining the organisation's governance and management framework (see 4.1)
- setting, communicating and implementing the organisation's government digital and data strategy and plans (see 4.2)
- ensuring continuous improvement of government digital and data activity is a priority within the organisation
- supporting integrated management of digital and non-digital aspects of services, working with the senior officer accountable for service delivery (see 4.6.7)
- managing government digital and data risk within the organisation's risk appetite and tolerance (see 4.5)

- ensuring AI-related risks are identified, owned, assured and managed within the organisation's risk appetite and legal obligations

The senior officer accountable for an organisation's government digital and data portfolio should be a member of the organisation's senior decision-making forums to ensure that government digital and data priorities, risks and dependencies are represented.

Note: In most organisations this role is, but not limited to, a Director or Director General.

Note: This role is often known as Chief Digital Officer or Chief Digital and Information Officer and would usually lead the organisation's Government Digital and Data function.

Note: See Government Functional Standard GovS 002: Project Delivery for more on portfolio, programme or project management.

4.6.5 Senior officer accountable for data in an organisation

The senior officer accountable for data in an organisation is accountable to the senior officer accountable for the organisation's government digital and data portfolio (4.6.4), for managing the organisation's data (see section 7) in relation to government digital and data activity.

The senior officer accountable for data is responsible for ensuring that the organisation:

- adopts and complies with relevant data and security requirements (see 4.1)
- develops, maintains and implements a data and information strategy and plan (see 4.2)
- assigns roles and responsibilities for the ownership and management of

data assets, including accountability for data quality and remediation of issues

- is enabled to use data to drive improvement in its productivity and services
- ensures data used for AI is suitable, lawful, secure, well-governed, appropriately documented and monitored for quality, bias and drift

In large, complex organisations, where use of data relates to discrete business areas with different legal or security requirements, accountability for managing a subset of the organisation's data may be separately delegated. In these cases, the data and information strategy and plan should explain how relevant interfaces are defined and managed. See section 7, Data Management.

Government Functional Standard GovS 007: Security shall be complied with, with respect to data and information security. In line with this, organisations should consider appointing a data protection specialist role.

Note: This role is often known as the Chief Data Officer.

Note: This role might also be accountable to the senior officer accountable for analysis in an organisation for analysis related activity. See Government Functional Standard GovS 010: Analysis.

4.6.6 Senior officer accountable for technology in an organisation

The senior officer accountable for government digital and data in an organisation is accountable to the senior officer accountable for the organisation's government digital and data portfolio (see 4.6.4), for managing the organisation's government digital and data solutions (see section 6), and for ensuring that the organisation:



Government Functional Standard

- adopts and complies with relevant government digital and data requirements and guidance (see 4.1)
- develops, maintains and implements a government digital and data strategy and plan (see 4.2)
- assigns appropriate roles and responsibilities for the ownership and management of government digital and data solutions
- has an appropriate approach to technical security and resilience
- ensures AI-enabled solutions are designed, procured, implemented and monitored in line with security, resilience, ethics, assurance and data protection requirements
- the organisation uses performance data and user feedback to understand how well services are performing in terms of usability and efficiency
- AI or automation used in service delivery is transparent, monitored, explainable where appropriate, and subject to meaningful human oversight for significant decisions
- accountabilities and responsibilities for each service are assigned, with service owners taking end-to-end responsibility (see 4.6.8)
- appropriate provision is made for users who are not using digital channels

This role should provide technical direction for the design and delivery of services (see section 5), ensuring that government digital and data solutions, including AI-enabled solutions, are appropriate, cost-effective, scalable, secure, resilient and operationally sustainable. See section 6, Government digital and data management.

Note: This role is often known as the Chief

Technology Officer. In large or complex organisations, it is often supported by a Chief Architect.

4.6.7 Senior officer accountable for service delivery

The senior officer accountable for service delivery is accountable to the accounting officer for directing the integrated management of the organisation's service delivery operations, ensuring that:

- the portfolio of services, including digital and non-digital elements, meets policy and organisational objectives

Where an organisation's portfolio of services is complex or very large, accountability for a sub-portfolio of services may be delegated (directly by the accounting officer, or from this role), provided the resulting user and product interfaces are defined and managed.

Note: In a government department or large arm's length body, with services comprising a mix of digital and non-digital components, it is likely that a Director General or Chief Operating Officer would be the appropriate person to undertake this role.

4.6.8 Service owner

The service owner is accountable to the senior officer accountable for service delivery (4.6.7) for the oversight and promotion of their assigned end-to-end service (see section 5), including:

- developing and operating the service holistically (covering digital and any non-digital elements) to meet user needs, operate efficiently, and maintain required levels of performance (see 8.9)

- maintaining a service backlog to support the setting of priorities for continuous improvements, enhancements and updates
- ensuring necessary approval processes are followed, and risks and issues are mitigated (see 4.5)
- ensuring AI-enabled service changes are tested, monitored and assured before and after deployment
- securing and managing costs and pricing, where appropriate
- managing customer relations and responding to user feedback (see 8.6)
- service transition and retirement, where necessary

The service owner is accountable for ensuring that relevant roles and responsibilities for delivery of the service are assigned and documented, and for the integrated management of the service across the multi-disciplinary delivery team.

The service owner should be supported by a digital service manager (see 4.6.9) to manage the specific digital aspects of the service. Where appropriate and justified, this role may be combined with the role of digital service manager to streamline operations, for example where a service is delivered only through digital channels.

4.6.9 Digital service manager

The digital service manager is responsible for the development and day-to-day operation of the digital aspects of their assigned service (see section 5), and is accountable to the service owner for:

- Ensuring the digital service meets user needs (see 8.3)
- managing digital content and design

- planning, tracking, reviewing and reporting on the operation of the digital service (see 5.4)
- ensuring there is useful and timely performance and management information data (see 5.6) on the services, and that this is consistent with cross-government standards
- prioritising and managing workflow
- responding to and resolving problems, incidents and issues
- escalating risks and issues as needed (see 4.5)
- delivering continuous improvements, enhancements and updates
- ensuring any AI-assisted operational activity is appropriately monitored, reviewed and escalated where risks, inaccuracies or service impacts arise

5. Service management

5.1 Overview

This section provides a framework for developing, managing, improving and, where needed, retiring services.

Services should be digital where this best meets user needs, and should be developed and delivered by multidisciplinary teams using agile methods.

Accountability for the ownership and management of service delivery and each service shall be assigned (see 4.6.7 and 4.6.8).

5.2 Policy intent

Policy intent should be reflected in the organisation's business strategy, business plan and service portfolio (see 5.5).



Service outcomes, efficiencies and benefits should be defined and traceable to the achievement of, or support for, policy intent.

Policy owners and those accountable for service delivery should work in cross-functional teams under a single service owner, so policy intent is reflected continuously.

5.3 Service design and development

New, changed or transformed services should provide value to government and users, and be usable and efficient. See GovS 002, Project delivery.

Services shall be delivered in accordance with the Service Standard. [2]

User research (see 8.3), iterative development and, where appropriate, testing of AI-enabled components should continue throughout the service life cycle.

Services shall be monitored using consistent service performance measures (see 5.6), reviewed quarterly.

Where services are not digital, or perform poorly against usability and efficiency measures, the service owner should consider redesigning the service end-to-end.

Organisations buying off-the-shelf products, services or AI-enabled tools should ensure suppliers can meet user needs and relevant standards. See 6.3 and GovS 008, Commercial.

Government Functional Standard GovS 007: Security shall be complied with by embedding cyber security into digital services, including any AI-enabled components, throughout the life cycle.

Note: Advice and guidance about technology choices can be found in the Technology Code of Practice. [3]

Note: Where AI is used in a service, it should be used only where there is clear evidence of user need, with appropriate human oversight, assurance, transparency, security and monitoring.

Note: The Service Manual includes advice on creating and running public services that meet the Service Standard. [11]

5.4 Service management

Services should be documented so their architecture, components and connections are defined and understood. This should include:

- user-facing and internal systems
- the people and the tasks they carry out to run the service
- processes
- data flows, decision points and any AI-enabled components

A target operating model should be developed and maintained for each service. It should set out the delivery approach (see 8.2), working practices and processes, people and skills, and the data, technology and AI capabilities needed to provide the service in line with government digital and data ways of working.

Integrated management should cover:

- digital and non-digital components of a service
- the service and the wider system of systems of which it is part, including dependencies on other organisations that provide parts of the same user journey

Services should be delivered and improved iteratively to meet changing user needs, developments in technology, including AI where appropriate, and changes in government policy, releasing value through frequent deployment cycles.

Service owners and teams should use qualitative and quantitative evidence, including performance analytics (see 5.6), user feedback, user research (see 8.3) and evidence from AI monitoring where relevant,

to prioritise iterative delivery and improvement. Improvements should be managed through a single service backlog.

5.5 Management of the organisation's portfolio of services

Organisations should maintain a service catalogue so public-facing and internal services, technologies and AI-enabled capabilities are discoverable for use and possible reuse across the organisation and by other organisations.

The portfolio of services should be maintained to ensure:

- technology, data, AI-enabled and non-digital components are planned and managed as a unified and consistent system
- there is a consistent portfolio-wide view of material risks, opportunities, concentrations of risk, inter-service dependencies and systemic vulnerabilities, with clear ownership and escalation arrangements
- user journeys across multiple services are streamlined and deliver a consistent user experience
- there is a consistent view of performance and prioritisation, as well as dependencies between services
- feedback informs future design and delivery across the organisation's services

5.6 Performance metrics and feedback

The service owner should define and collect performance metrics, taking account of the cross-government performance framework and any additional assurance needed for AI-enabled components.

Service performance targets should be established, managed and aligned with cross-government performance metrics. They should include:

- data on usability and efficiency of the service
- meeting defined service levels
- accuracy, reliability, bias, transparency and human oversight measures where AI is used

Performance against targets should be reported to senior leaders and stakeholders, and should meet requirements in the cross-government governance and management framework (see 4.1).

5.7 Accessible and inclusive services

Accessible and inclusive services ensure any potential user can use the service regardless of their personal characteristics, situation, capabilities or access needs, and has equal access and opportunity.

Digital services shall be designed and managed to meet defined user abilities and accessibility requirements. Relevant legislation shall be identified and must be complied with, including where AI affects access, decisions, content or user support.

Those accountable for service development and delivery should:

- build services that are intuitive to use, and present complicated information as simply as possible



- consider and address the barriers different groups of users might face when trying to use the service
- encourage users to use digital services, while providing help, human support and non-digital alternatives for those without the skills or access to use the digital option
- make sure users know which channels are available to them

Note: Guidance on making services inclusive can be found in the Service Manual. [11]

Note: The Service Standard sets requirements for accessibility, usability, consistency and efficiency. [2]

Note: Attention is drawn to the public sector accessibility regulations. [12]

5.8 Service retirement

The senior officer accountable for the organisation's service delivery (see 4.6.7) may decide to retire a service, taking advice from the service owner. This might reflect changes in policy or user need, consolidation with another service, or replacement of legacy technology, including AI-enabled components where relevant.

Once the decision to retire a service has been taken, the service owner should:

- archive or move relevant assets
- inform and support the public or business users to migrate to any new service
- consider dependencies across and beyond the organisation's service portfolio, including data, technology and AI dependencies
- ensure impacted stakeholders are engaged

- review and, where needed, decommission AI models, prompts, data pipelines and monitoring arrangements safely

6. Technology management

6.1 Overview

A senior officer accountable for government digital and data shall be assigned in each organisation (see 4.6.6).

The senior officer should ensure insights, research, data, technology and emerging capabilities, including artificial intelligence (AI), inform the organisation's strategy, architecture and asset management approach (see 8.8).

Government Functional Standard GovS 002: Project Delivery shall be complied with, with respect to work that is part of a portfolio, programme or project.

AI should be considered as part of the wider government digital and data landscape where it supports user needs, public value, operational effectiveness or better decision-making. Any use of AI should be lawful, ethical, secure, transparent and subject to appropriate human oversight, assurance and risk management.

Relevant strategy, policy and subject specific standards should be followed, including:

- The Technology Code of Practice [3]
- Cloud First Strategy [13]
- Managing Vendor Lock-in [14]
- National Institute of Standards and Technology [15]
- Cyber Essentials [16]

6.2 Technology development and maintenance

Digital and data architecture sets the parameters for the configuration, interaction and interdependence of the components, services, data assets and systems that enable government digital and data solutions.

Architecture should align with the relevant target operating model, service needs and data requirements (see 5.4 and 8.4).

Digital and data architecture should reflect the organisation's government digital and data strategy, support current and future service delivery, and remain deliverable within the organisation's risk appetite (see 4.5).

In keeping with the published standards (see 6.1), government digital and data solutions should:

- be secure by design
- use open standards and open code
- adhere to relevant classification standards
- protect data at rest and in transit
- include appropriate governance, assurance and lifecycle controls where AI capabilities are used

Government digital and data products, services and systems should be understood and actively managed. Governance controls should reduce legacy technology, manage technical debt, track cross-government alignment, understand supplier and supply chain dependencies, and avoid unnecessary duplication. Controls should also cover business continuity, resilience and, where AI is used, model performance, data quality, bias, security, transparency, accountability and ongoing assurance.

Organisations should identify, document and manage risks and dependencies, including external dependencies and supply chains, especially where shared services, shared data arrangements or AI-enabled capabilities are in place (see 4.5).

Government digital and data solutions may be developed and managed in-house, by third-party suppliers, or through a combination of both. Where AI components are procured, built or integrated, roles, responsibilities, assurance requirements and supplier obligations should be defined from the outset (see 4.5).

6.3 Deployment and operation of technology

6.3.1 Overview

Each organisation should have mechanisms for managing and continually improving its government digital and data solutions, so that changing business, policy, operational and user needs continue to be met.

Relevant roles and responsibilities should be defined and assigned to reflect the organisation's build or buy choices, including responsibility for AI-enabled components where applicable (see 4.5).

Government Functional Standard GovS 007: Security shall be complied with, with respect to a mechanism being in place for identifying and resolving security vulnerabilities.

Note: For buy (third-party delivery), responsibilities are defined in the contract; for build (in-house delivery) see Technology Code of Practice guidance. [3]

6.3.2 Operations management

The senior officer accountable for government digital and data (see 4.6.6) should ensure those managing digital and data solutions have the capability, capacity



and defined processes to run, operate and continuously improve them.

Processes should be defined and managed, and responsibility assigned for:

- ensuring clean, secure and maintainable code for the organisation
- maintaining, iterating, and patching solutions against known vulnerabilities
- understanding, identifying and remediating potential risks, with effective operational monitoring, including relevant service management processes such as incident management, problem management and disaster recovery
- ensuring consistent and tested business continuity arrangements are in place and understood by all stakeholders
- monitoring AI-enabled components where used, including performance, drift, data quality, security risks, explainability, human oversight and escalation routes

6.3.3 Triggers for change

Triggers for change should be understood and managed. They are likely to relate to:

- internally generated change derived from operating digital and data solutions, including user feedback, data insights and performance metrics
- externally generated change derived from a new or updated policy, a public announcement, supplier expiry or another external reason

- change generated from decisions taken about the organisation's digital and data architecture (see 6.2)
- changes in AI capability, regulation, risk profile, model performance, data quality or assurance requirements

Addressing triggers for change might result in incremental change, service improvement, technical remediation, or upgrades managed through a project or programme.

The organisation's legacy technology, data stores, digital services and AI-enabled components should be defined and monitored. An up-to-date plan should be maintained to remediate, replace or retire them.

Technology, data stores, digital services or AI-enabled components become legacy when they meet any of the following conditions:

- considered an end-of-life product
- out of support or on extended support from the supplier
- impossible to update
- no longer cost-effective
- considered to be above the acceptable risk threshold
- no longer meet required levels of assurance, explainability, data quality, security or human oversight

6.4 Retirement of government digital and data solutions

6.4.1 Overview

The purpose of retirement is to ensure government digital and data solutions remain fit for purpose. A solution should be considered for retirement if:

- it is not possible to update or improve the existing solution to meet future business, policy, operational or user needs
- there are resource constraints
- the solution represents poor value for money
- there is a reduction or ending of future supplier support
- identified risks are unacceptably high
- it is incompatible with the ambition set by the organisation's government digital and data strategy
- AI-enabled components can no longer be assured, monitored, explained, secured or controlled to an acceptable standard

The senior officer accountable for government digital and data in an organisation (see 4.6.6) should:

- identify components, systems, data stores or services that are no longer capable of meeting the organisation's needs
- identify the services or business operations that rely on the solution intended for retirement
- consult service owners, data owners and other stakeholders that rely on the existing solution, to understand their priorities for future operation
- assess whether any AI-enabled components, models, training data, prompts, outputs, logs or derived data need to be retained, migrated, archived or deleted
- oversee service delivery teams to ensure the management and retirement of the solution and, where

necessary, its replacement, meets the organisation's needs

- work with service owners and stakeholders to ensure all data is migrated, archived or removed in line with data protection, classification and information assurance requirements
- lead the removal and appropriate disposal of retired technology, systems and data assets

Necessary replacement arrangements should be in place before retirement takes place.

Note: Retire includes withdrawal from existing services or operations, and disposal of associated technology, systems, data assets and AI-enabled components.

6.4.2 Withdraw technology

The process and complexity of moving away from legacy systems, data stores, technologies and AI-enabled components varies depending on the solution involved.

Note: For example, decommissioning physical hardware such as laptops is more straightforward than decommissioning a mainframe and building a replacement system in the cloud.

Before a solution is withdrawn, the following actions should be taken:

- review existing contractual arrangements and take any necessary action to end the contract, if appropriate
- prepare data that is to be migrated
- plan transition of services to alternative solutions, if required
- define and implement a secure process for migrating data between systems, or data removal and



destruction based on the information assurance needs and any GDPR data associated with the system

- confirm whether any AI models, configuration, prompts, outputs, logs, training data or evaluation records need to be retained, transferred, archived or securely destroyed
- engage with staff and other users affected by the change, and provide necessary training or guidance

6.4.3 Dispose of technology, systems and data assets

The service owner (see 4.6.8) and the senior officer accountable for government digital and data in an organisation (see 4.6.6) should ensure redundant equipment, systems, data assets and AI-enabled components are appropriately disposed of.

Disposal shall meet security requirements, and any physical hardware disposal should, where possible, be recycled using recognised and sustainable approaches.

When decommissioning cloud-based assets or AI-enabled services, processes should ensure residual data, models, logs, outputs and configuration are not accessible post disposal. Relevant security guidance should always be considered when disposing of technology.

Requirements for the handling of personal data being moved or removed must be followed in accordance with prevailing regulations and security advice, including where personal data has been used in AI-enabled systems.

Note: Attention is drawn to the following requirements:

- UK General Data Protection Regulation (UK GDPR) [17]
- The Data Protection Act [18]

Government Functional Standard GovS 007: Security shall be complied with when disposing of technology, systems, data assets and AI-enabled components.

Where AI-enabled components are retired or disposed of, organisations should ensure models, prompts, outputs, logs, training data, evaluation records and configuration are handled in line with data protection, security, information assurance and retention requirements.

7. Data management

7.1 Overview

This section sets expectations for managing data as a strategic asset that supports better public services, evidence-based decisions, operational effectiveness and responsible innovation across government, including the safe and transparent use of artificial intelligence.

Each organisation shall assign senior accountability for data, with clear ownership for data strategy, governance, quality, protection, ethical use, sharing and reuse (see 4.6.5).

Organisations should follow cross-government strategies, standards and governance for government digital and data, including guidance from the Data Standards Authority, the Government Data Quality Framework, the Data and AI Ethics

Framework, the Algorithmic Transparency Recording Standard, and relevant security, privacy and technology standards (see section 4).

Data should be retained, archived or disposed of in accordance with the organisation's retention schedule, information management policy, security requirements and legislation.

Note: The National Data Library is the home of UK public data to inform decisions and build services. [5]

Note: Attention is drawn to:

- UK General Data Protection Regulation (UK GDPR) [17]
- The Data Protection Act [18]
- Public Records Act [19]
- Freedom of Information Act [20]

7.2 Data management principles

Data management must be lawful, ethical, secure, transparent and proportionate to the purpose for which data is collected, used, shared and retained.

Organisations should ensure their data is fit for purpose by:

- identifying critical data and information assets, including those needed for service delivery, policy, operations, analysis, reporting, cross-government sharing and AI-enabled services
- assigning accountable owners and stewards for critical data and information assets, with clear responsibilities for governance, quality, access, protection, retention, disposal and lifecycle management
- maintaining metadata and catalogues so that data can be found, understood, validated, reused and shared appropriately
- putting processes in place to identify, prioritise, remediate and monitor data quality issues at source

Organisations should ensure their data is trusted, accessible and reusable by:

- being able to evidence that critical data assets meet minimum standards for governance, quality, security,

privacy and ethical use, based on their purpose and context

- ensuring data is discoverable through maintained catalogues, with clear metadata, lineage, quality information and access conditions
- applying appropriate security, privacy, access and information assurance controls so data can be shared safely and lawfully

Organisations should ensure their data architecture (see 7.4) supports interoperability, reuse and secure exchange by:

- identifying authoritative sources for critical data and ensuring they are appropriately governed, maintained and provisioned
- using open standards, common data models and agreed reference data where appropriate to improve consistency and interoperability
- being able to evidence that application programming interfaces (APIs), data exchange platforms and analytical environments meet appropriate standards for governance, security, privacy and control
- documenting classifications, sensitivity, criticality, retention requirements, lineage and usage restrictions so data is handled appropriately
- maintaining integrated catalogues for data, interfaces, standards and data sharing arrangements
- ensuring data used to train, test, validate or operate AI systems is documented, lawful, representative, secure and appropriate for the intended use



There should be accountable ownership for data quality, protection, security, ethics, access, sharing and reuse, supported by cross-government guidance, frameworks and standards.

To support continuous improvement and help senior leaders prioritise investment, organisations should assess data maturity across technical, governance, cultural, skills and leadership factors using an appropriate framework.

Throughout the planning, implementation and evaluation of projects, programmes, services, analytical work and AI-enabled solutions, organisations should use the Data and AI Ethics Framework to ensure data and AI are used appropriately, responsibly and transparently. [21]

See Government Functional Standard GovS 002: Project Delivery.

Where specified, publication of data and analysis should be done through approved routes. For example, publication of official statistics should follow the protocols set out in the Code of Practice for Statistics, which provides the framework for trustworthy, high-quality and valuable statistics. These principles are relevant across data management and should be followed where appropriate. [22]

Note: The Data Standards Authority exists to improve how the public sector manages data, including by setting standards for sharing and using data across government. [23]

Note: The government's Data and AI Ethics Framework guides appropriate and responsible use of data, data-driven technologies, automated decision-making and AI in government and the wider public sector.

It helps public servants identify ethical considerations, manage risks and maintain trust across the lifecycle of data and AI projects.

7.3 Data frameworks and operating models

Organisations shall follow appropriate guidance when implementing data frameworks and operating models, including for cross-government data sharing,

business intelligence, artificial intelligence, machine learning, automation and advanced analytics.

Note: The following products provide best practice guidance:

- Principles for securing personal data in government services [24]
- AI Playbook for UK Government [25]
- Data and AI Ethics Framework [21]
- The Algorithmic Transparency Recording Standard [26]

7.4 Data architecture

Data architecture describes the systems, processes, standards, models and structures used to acquire, create, move, store, query, protect, share, archive and dispose of data to meet user, service and business needs.

Organisations need confidence that the right data is available when needed, in usable, accessible, secure and standardised formats, and that data and system capabilities meet user, service and operational needs.

When developing data architecture proposals, organisations should follow relevant standards, guidance and tools, including open standards, API standards, security guidance, data protection requirements, AI assurance guidance and guidance on managing data assets (see 8.8).

Note: For practical advice, see the data management capability framework and the

GOV.UK collection of design guidance for application programming interfaces. [27]

The following web-based API standards guidance will help your organisation deliver the best possible services to users:

- UK Government Reference Architecture for Data and APIs [28]
- GraphQL Guidance - an API specification originally developed by Facebook as an alternative to REST for querying complex data structures [29]
- API Management Guidance - enabling you to standardise how teams design, launch and manage APIs in your organisation [30]
- Domain Guidance for api.gov.uk - contact the Government Digital Service to get a domain for your API on GOV.UK [31]

7.4.1 Managing data quality

Data quality should be measured using dimensions such as completeness, uniqueness, consistency, timeliness, validity and accuracy. The dimensions and thresholds used should reflect the intended use, risk, sensitivity and impact of the data, including where data supports AI or automated decision-making.

Organisations should develop a culture of data quality, by:

- treating issues at source and committing to ongoing monitoring, reporting and continuous improvement
- targeting improvements where they add the most value or reduce the greatest risk
- managing data quality proactively across the data lifecycle

- making data quality visible to users through metadata, quality statements or other appropriate information

A data quality action plan may be used to manage improvement work. If used, it should identify owners, priorities, root causes, actions, measures, timescales and reporting arrangements, and should be reflected in the organisation's information and data plan (see 8.5).

Organisations should use measurable characteristics to improve data quality, and should:

- maintain an assessment of the current level of data quality
- set targets for appropriate quality levels in the future
- monitor quality to ensure that planned improvements are made

Such quality measures should ensure that accountability is clear (see 4.6.5) and that:

- quality characteristics are assessed in relation to a specific use at various points
- the impact of changes to relevant data collection, storage, and processing is assessed

Note: The Data Quality Hub provides information and support on data quality. [32]

Note: Further information and guidance can be found in the Data Quality Framework. [33]

7.5 Data and information asset management

Data and information asset management enables an organisation to identify, record, understand, govern and maintain its data and information assets so it knows what it holds, where it is held, who is accountable



for it, how it can be accessed, how it should be protected, and how it is retained, reused, shared or disposed of.

Organisations should follow existing standards and guidance, including the data asset management policy where applicable, and should manage data so that:

- critical data and information assets are identified, recorded, maintained and reported where required
- metadata is actively managed to describe data and information assets, ownership, quality, lineage, sensitivity, retention, disposal and access conditions
- data is shared by default where lawful, ethical, secure and appropriate, and where there are no valid reasons not to share
- data is reused to maximise value and minimise unnecessary duplication, collection and storage
- dataset linkage is managed safely, with appropriate privacy, security and ethical controls
- access permissions are strictly managed and reviewed regularly
- data governance, security, privacy and compliance requirements are observed throughout the data lifecycle
- interoperable data infrastructure, open standards and integrated catalogues are used where appropriate
- data assets used in AI systems are recorded with their purpose, provenance, quality, limitations, access conditions and retention requirements

Note: For information asset ownership, see government guidance on the Information Asset Owner role. [34]

Note: The resources listed provide best practice for managing and supporting data asset management:

- API Catalogue [35]
- Reference Data for Use Across Government [36]
- Address Base Guidance - use free property and street information to add geospatial data to your projects and comply with the UPRN standard [37]

7.6 Data engineering

The purpose of data engineering is to make data useful, accessible, reliable and secure for authorised users so they can make informed decisions, improve services and optimise organisational performance.

Data engineering includes acquiring, ingesting, validating, transforming, modelling, documenting, storing, securing and provisioning data in formats that meet user needs and support safe reuse, including for analytics, automation and AI where appropriate.

To ensure useful and accessible data through data engineering, organisations should:

- follow cross-government data standards, open standards and agreed reference data where appropriate
- produce, maintain and update data models, pipelines and documentation for specific user, service and analytical needs
- maintain metadata repositories, catalogues and governance

arrangements for the data they create, transform and provision

- apply quality checks, monitoring and controls across the data development lifecycle
- design data pipelines and platforms to be secure, resilient, scalable, sustainable and maintainable
- maintain appropriate controls for AI-related data pipelines, including versioning, monitoring, reproducibility, auditability and safeguards against inappropriate or unauthorised use

8. Digital management practices

8.1 Overview

These practices support the development, delivery, operation and continuous improvement of sustainable government digital and data activity, including the responsible use of artificial intelligence (AI) where it is used in products, services or internal processes. They apply across the scope of this standard.

Managers responsible for government digital and data activity, supported by subject matter experts where needed, should plan, manage and monitor work so that:

- delivery approaches are defined and assured (see 8.2)
- policy and business outcomes are met through user-centred, accessible and inclusive design (see 8.3)
- digital components, data and AI-enabled systems are integrated or interoperable where appropriate (see 8.4)

- knowledge, information and data are managed appropriately (see 8.5)
- channels, user engagement, sustainability, assets, performance, reporting, capability, risk, procurement and contracts are managed effectively (see 8.6 to 18.12)

8.2 Delivery approach

8.2.1 Choose the right delivery approach

A delivery approach sets out how a solution is designed, delivered, implemented, operated, improved and decommissioned. For most government digital and data activity, the default should be agile, iterative and product-centred where appropriate, including where AI is being explored or used.

The person leading the work, such as a service owner, should define an approach that:

- assures quality, control and compliance with relevant standards and guidance
- identifies the skills, data, technology and supplier support needed
- considers specific assurance, security, ethical and human oversight requirements where AI is used.

The approach should reflect:

- whether the work is new or an enhancement to an existing product or service
- confidence in user needs, business requirements, data quality and technology choices
- timescales, outputs, risks and whether value can be delivered incrementally



Different approaches may be used for different components of a wider system, provided they:

- integrate at appropriate points
- manage overall system risk
- align with government digital and data architecture, standards and patterns

Agile techniques, behaviours and incremental releases should be used where they deliver early user value, support learning and enable continuous improvement.

Services (see section 5) shall be delivered in accordance with the Service Standard. [2]

8.2.2 Agile delivery approaches

Agile delivery approaches are adaptive, iterative and incremental, and include:

- behaviours and culture
- methods and techniques
- management frameworks

Agile approaches should be used where rapid value creation, learning and flexibility are needed, and should normally be adopted for government digital and data activity unless a predictive approach is justified (see 8.2.3).

Agile culture and multi-disciplinary teams should support continuous improvement, delivery milestones and safe experimentation with emerging technologies, including AI.

Guidance about how to embed routine benchmarking of the organisation's digital maturity should be followed.

See Government Functional Standard GovS 002: Project Delivery.

8.2.3 Predictive delivery approaches

Where appropriate, a predictive delivery approach may be used instead of agile delivery.

Predictive approaches may be appropriate where incremental release is not feasible or would introduce unacceptable risk, for example:

- large capital infrastructure projects
- complex infrastructure remediation programmes
- tightly coupled legacy systems
- safety-critical systems where test-and-learn would create substantial risk

Note: Waterfall is a traditional software development approach and an example of a predictive, rather than iterative, approach. It is characterised by a sequential delivery where one step in delivery is completed before starting the next. Typically, this comprises requirements, design, development, testing, and deployment.

8.3 User-centred design

User-centred design ensures digital products and services meet current and future user needs in an accessible, inclusive and timely way, while supporting policy and business outcomes. AI should be used where there is clear evidence that it meets user needs and improves outcomes.

Note: Attention is drawn to the public sector accessibility regulations. [11]

User needs should be:

- identified, understood and used to inform design and objectives
- balanced with policy, business, accessibility and inclusion outcomes

- supported by transparency where AI affects data, decisions, outputs or user experience

User needs should be used to design digital products and services that are simple, accessible, inclusive and efficient, enabling users to achieve their goals more easily than current practices allow.

Note: A user might be a member of the public, a person representing businesses or organisations, specific professionals, or anyone working within or for government (including third-party suppliers).

8.4 System integration and interoperability

Reusing technology, data, standards, patterns and common components, and designing for interoperability, reduces duplication, supports value for money and enables coherent user experiences. AI-enabled components should be designed to integrate safely and transparently with wider systems.

Organisations should develop and maintain catalogues for services, data, technology and reusable components where these are needed to support discovery, reuse, assurance and effective management.

Catalogues should include public-facing and internal information, so that their content is discoverable and can be used or reused across the organisation and, where appropriate, by other government organisations.

8.5 Knowledge and information management

Knowledge and information management ensures that knowledge, information and data are available, reliable and usable for The organisation's knowledge and information requirements should be understood and documented. Critical information and data should be identified in

the organisation's digital and data strategy, and reflected in the organisation's plans (see 4.2.2) and asset management arrangements (see 8.8).

Organisations should define accountabilities for the ownership, protection, use, retention and disposal of information and data assets. This should include appropriate roles such as Information Asset Owners, Data Owners, Departmental Records Officers and the senior person accountable for information security risk, in line with organisational governance and relevant government guidance. Departmental Records Officers should help ensure compliance with records management and information management requirements, including the retention, disposal and transfer of official records.

Government Functional Standard GovS 007: Security shall be complied with, with respect to data and information security.

8.6 Use of channels and user engagement

A channel is the medium to deliver information or a service to an end user.

For each service and across the service portfolio, organisations should understand:

- channel usage, costs and transitions between channels
- which channels are needed by different user groups
- how failures in one channel affect demand on others
- how services, including AI-assisted channels, remain accessible, inclusive and clear about when users are interacting with automation

Where user journeys are omnichannel, service owners should consider both usability and efficiency in their design.



Users' feedback should be collected and managed. Where possible, users should be kept proactively informed of progress of the service, to reduce demand for updates.

A complaints procedure should be defined. Complaints should be resolved or explained in a timely way.

8.7 Sustainability

Digital products and services should be designed, delivered and operated sustainably. This includes considering the environmental impact of technology choices, data storage, infrastructure and AI systems, as well as their resilience to climate risk.

Sustainability requirements should be a key component of design, delivery and implementation as well as evaluation scores in procurement exercises. They should be included in the objectives and scope for the digital solution and should be documented.

Organisations should adopt a circular and efficient approach to digital services and technology, by reusing common platforms, removing duplicate data and redundant services, and extracting value from end-of-life assets in line with the waste hierarchy.

The management of environment and sustainability should be covered in or referenced from a service's defined delivery approach, if not already covered in organisation-wide policies and procedures. Relevant legislation shall be identified and must be complied with.

Note: See the Defra digital sustainability strategy 2025 to 2030 as an example departmental strategy for this topic. [38]

8.8 Configuration and asset management

8.8.1 Overview

Configuration management ensures that the assets needed to test and deliver a product or service are:

- working consistently together
- controlled in a consistent manner
- accurately and reliably documented
- subject to two-way traceability

The approach to asset management should be included in digital and data strategies (see 4.2).

Asset management plans should:

- support effective control across the government digital and data portfolio, including technology, data, models, AI components, tooling and legacy assets
- processes and frameworks to build stable and scalable systems
- use of configuration management tools
- use of common and interoperable tools across different projects and stages

These plans should include expectations for future management of assets relating to legacy technology and services.

8.8.2 Manage technology assets

Technology assets should be managed throughout their life cycle to:

- reduce overall costs through retirement of redundant technology
- manage technical debt

- track technical alignment with other organisations
- understand vendor usage and supply chain

8.8.3 Manage data assets

Data assets should be managed throughout the data life cycle so organisations understand what data they hold, where it is held, who can access it, how it is handled and whether it is suitable for reuse, analytics or AI. Organisations should maintain:

- what data is held by the organisation
- how and where the data is held
- who has access to what data, in what circumstances
- the handling arrangements for specific data

Guidance for data collection should be followed, including a controlled and consistent process for obtaining or importing data. Organisations should:

- keep an original copy of data
- back it up
- maintain metadata
- keep an audit trail
- enable rollback where appropriate
- actively manage data quality

Data should be retained only where necessary, and for the minimum period in line with policies, guidance or with the agreements in place with data suppliers or providers.

Metadata is information about the characteristics of the data, and how the data should be handled.

8.9 Performance management

Organisations should align with relevant cross-government performance frameworks to measure and report service performance, technology estate health, digital and data capability, organisational maturity and, where relevant, the performance and impact of AI-enabled systems.

8.10 Management information, analytics and reporting

Management information should be accurate, complete and timely so people can undertake their roles and make informed decisions.

Workflows, dashboards and standard reports should support monitoring, decision making and reporting. Where analytics or AI are used, outputs should be explainable, reliable and subject to appropriate human oversight.

Standard, consistent reports should be available directly from the management information system to support internal and external activity, decision making and reporting.

Appropriate data should be retained in accordance with the organisation's data retention policy and prevailing legislation.

8.11 Digital capacity and capability

Digital and data capacity and capability management balances supply and demand for skilled people, equipment, tooling, facilities and supplier support. This includes the capability needed to design, buy, use, assure and govern AI safely and effectively.

Organisations should maintain a view of current and future skills needs, address shortfalls, re-plan work where resources are constrained, and put business continuity measures in place for critical resources.



Where third parties provide better value, they should be used in line with relevant commercial, digital and data guidance, including the blueprint for modern digital government. [39]

Organisations should capture third-party use and associated skills in capacity and capability plans.

Senior civil servants within an organisation shall be assessed against the Digital and Data Essentials standard. [40]

Government Functional Standard GovS 003: People shall be complied with, with respect to people management.

18.12 Purchasing and contract management

18.12.1 Procurement

Organisations shall decide whether service solutions or components should be built internally, supplied by a third party, reused from existing government solutions, or delivered through a combination of approaches.

Purchasing strategies should support commercial, contractual, technology, data and AI considerations, including whether existing products or government solutions can meet the need.

Decisions should take account of insights and research and should reflect that, where possible, commercial off-the-shelf products or existing solutions already in use across government should be used.

Building or tailoring a solution should only be considered where:

- user need is unique or rare
- supplier options are limited
- commercial products cannot be scaled, adapted or assured to meet the need

- there are clear reasons to own, modify or control the technology, data or AI model

An assessment of resources should be made to inform build or buy decisions, such as staff and funding, skills, operational capacity and the ability to deliver ongoing training.

Government Functional Standard GovS 008: Commercial shall be complied with, with respect to procurement and management of contracts.

Note: See Should Cost modelling for purchasing strategy guidance. [41]

18.12.2 Contract management

A contract management plan should define each party's roles and responsibilities and be reviewed throughout the contract. For AI-enabled products or services, it should also cover transparency, security, data use, intellectual property, performance monitoring, assurance and exit arrangements.

Government Functional Standard GovS 008: Commercial shall be complied with.

A. References

All references are correct at the time of publication; users should check for updated versions.

ID	Description
1	Functional Standards – GOV.UK, Functional Standards (2021)
2	GOV.UK, Service Standard
3	Central Digital and Data Office, The Technology Code of Practice (2025)
4	Central Digital and Data Office, Transforming for a digital future (2022)
5	Department for Digital, Culture, Media and Sport, National Data Library (2026)
6	UK Government Security, GovAssure (2026)
7	Functional Standards – GOV.UK, Government Functional Standard GovS 009: Internal Audit (2026)
8	HM Treasury, Orange Book: Management of risk - Principles and Concepts
9	Central Digital and Data Office, Cabinet Office Controls (2026)
10	HM Treasury, Managing Public Money (2022)
11	GOV.UK, Service Manual
12	Central Digital and Data Office, Understanding accessibility requirements for public sector bodies
13	Central Digital and Data Office, Government Cloud First policy (2023)
14	Central Digital and Data Office, Managing technical lock-in in the cloud (2015)
15	National Institute of Standards and Technology
16	National Cyber Security Centre, Cyber Essentials
17	UK General Data Protection Regulation
18	Data Protection Act
19	Public Records Act
20	Freedom of Information Act
21	Government Digital Service, Data and AI Ethics Framework (2025)
22	Code of Practice for Statistics (2025)
23	Data Standards Authority
24	GOV UK, Principles for securing personal data in government services (2025)
25	Government Digital Service, Artificial Intelligence Playbook for the UK Government (2025)
26	Central Digital and Data Office, Algorithmic Transparency Reports (2025)
27	Central Digital and Data Office, Government Digital and Data Profession Capability Framework (2026)



28	Central Digital and Data Office, Develop your data and APIs using a reference architecture (2021)
29	Central Digital and Data Office, Using GraphQL for your API (2021)
30	Central Digital and Data Office, Defining an API management strategy (2021)
31	Central Digital and Data Office, Get an API domain on GOV.UK (2021)
32	Office for National Statistics, Government Data Quality Hub
33	Government Data Quality Hub, The Government Data Quality Framework (2020)
34	Government security, The role of information asset owners in government (2025)
35	Central Digital and Data Office, UK public sector APIs
36	Central Digital and Data Office, Publish reference data for use across government (2021)
37	Central Digital and Data Office, Access free address data using AddressBase
38	Department for Environment, Food and Rural Affairs, Defra digital sustainability strategy 2025 to 2030 (2025)
39	Policy paper - A blueprint for modern digital government (2025)
40	Central Digital and Data Office, Digital and Data essentials for senior civil servants (2023)
41	Government Commercial Function, Should Cost Modelling (pdf, 729 kb) (2021)

B. Glossary

See also the [common glossary of definitions](#) which includes a list of defined terms and phrases used across the suite of government standards. The glossary includes the term, definition, and which function owns the term and definition.

Term	Definition
algorithmic transparency	The practice of being open about where and how algorithmic tools are used, including their purpose, impact and governance.
application programming interface (api)	A set of rules and protocols that allows different software applications or systems to communicate with each other.
artificial intelligence	Technologies that perform tasks normally requiring human intelligence, such as learning, reasoning, prediction, classification or decision support.

application (digital)	A system for collecting, saving, processing, and presenting data by means of a computer. Note: The term application is generally used when referring to a component of software that can be executed.
architecture (digital)	Fundamental concepts or properties of a system in its environment embodied in its components, relationships, and in the principles of its design and evolution. Note: The term can be applied to any aspect of digital services, including service, data and technology.
cloud services	Computing services, such as storage, platforms, software or infrastructure, delivered over the internet and accessed on demand.
catalogue	Structured information about aspects of a service or its components. Note: Examples include service catalogue (services offered or provided by a service provider), data catalogue, application catalogue, interface catalogue.
channel strategy (digital)	A strategy to define the medium used to deliver a message to users of a service. Note: The channel can be a digital medium (such as a website or app), or a non-digital medium (such as a face-to-face appointment).
configuration item	A component of a service or system that needs to be managed to deliver, maintain or support that service or system.
data	Information that is collected, stored, processed, shared or used to support decisions, services and operations.
data quality	The degree to which data is accurate, complete, timely, consistent and fit for its intended purpose.
data standard	An agreed specification for how data is defined, structured, recorded, exchanged or managed.
digital	Modern technology-enabled processes, business models, tools and ways of working.
digital asset	Anything that is stored digitally and is uniquely identifiable. Note: Digital assets can include data and technology assets.



Government Functional Standard

digital product	A software application that has one or more capabilities.
digital technology	Digital technologies are electronic tools, systems, devices and resources that generate, store or process data. They comprise both hardware and software components.
digital transformation	The modernisation of technology, use of data, redesign of end-to-end processes, and more integrated ways of working to achieve improved services and business operations.
disaster recovery	A set of defined activities related to how an organisation plans to recover from a disaster and return to a pre-disaster condition.
event (digital)	A change of state that has significance for the management of a service or other configuration item.
incident (digital)	In the context of digital services, an incident is an unplanned interruption to a service or reduction in the quality of a service.
interoperability	The ability of systems, services, organisations or data to work together and exchange information effectively.
legacy (digital)	A service or component part of a service which is no longer considered fit for purpose.
life cycle	The stages through which a service, product, system, data asset or technology asset passes, from planning and design through delivery, operation, improvement and retirement.
minimum viable product	A service with just enough features to satisfy early users, and to provide feedback for future service development.
omnichannel	Different channels integrated into a single user experience.
open standard	A standard that is publicly available and can be used by anyone, supporting consistency, interoperability and reuse.

product-centric delivery (digital)	Products, capabilities and services that are delivered by a line of business or multiple lines of business together, which are often grouped around an end-to-end customer journey.
problem	A cause, or potential cause, of one or more incidents.
reference architecture	A common structure, model or set of patterns that supports consistent design and implementation across related services, systems or data.
release	A version of a service or other configuration item, or a collection of configuration items, that is made available for use.
reliability	The ability of a service or other configuration item to perform its intended function for a specified period or number of cycles under specified conditions.
resilience (digital)	The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs. Source: Taken from The NIST Definition of Cloud Computing.
retirement	Permanent withdrawal of a digital service or other configuration item from use.
roadmap	A high-level plan that sets out the intended direction, outcomes, milestones and major activities needed to achieve an agreed strategy or objective.
secure by design	The discipline of embedding cyber security into digital systems and services at every step of their life cycle - from the planning of a service to the procurement and configuration of technology and retirement at end of life.



Government Functional Standard

service	A service captures all the things that collectively deliver an outcome for users. Note: A service is a complete solution that brings together technology and non-technology elements to enable users to achieve a defined outcome.
service owner	The person accountable for the overall quality, operation and continuous improvement of a service.
service backlog	A list of new features, changes to existing features, bug fixes, infrastructure changes or other activities that a team may deliver to achieve a specific outcome. It is the single authoritative source for things that a service team works on.
service level	One or more metrics that define expected or achieved service quality.
service level agreement	Documented agreement between a service provider and users of a service that identifies the service provided and expected performance. Note: A service level agreement can be included in a contract or another type of documented agreement.
sustainability	The practice of designing, delivering and operating digital services and technology in a way that reduces environmental impact and supports long-term value.
technical debt	The implied cost of additional refactoring caused by choosing an expedient solution to deliver a piece of functionality or project instead of using an approach that would take longer or cost more. Note: This is typically calculated as the value of the hours required to refactor a piece of functionality or a project.
technology code of practice	A set of government guidance that helps organisations design, build and buy technology that is secure, sustainable, interoperable and aligned with user needs.

two-way traceability The ability to trace both forward and backward (for example, from a requirement to an element of the solution and from the solution element back to the requirement).

Note: Two-way traceability can also be applied in other areas, such as to output-outcome-benefits mapping, and solution-plan mapping.

Note: Two-way traceability is managed using configuration management.

user A person whose needs are to be met by a product, service or process.

Note: Users have a direct relationship with the product, service or process and might be end-users (such as a member of the public or a government official) or other users (such as those who maintain the product, service or process).

user experience How a user interacts with and experiences a product, system, or service.

user-centred design A framework or process that focuses on putting users at the centre of service or product design and development.

user journey A sequence of events or experiences a user can encounter while using a product or service.

user need Prerequisites identified as necessary for a user, or a set of users, to achieve an intended outcome, implied or stated within a specific context of use. Note: A user need is independent of any proposed solution for that need.

Note: User needs are identified based on various approaches, including interviews with users, observations, surveys, evaluations, expert analysis, etc.

Note: User needs often represent gaps (or discrepancies) between what should be and what is.

Note: User needs are transformed into user requirements by considering the context of use, user priorities, trade-offs with other system requirements and constraints.



validation	An activity that ensures a solution (or part of) meets the needs of the business. Validation ensures that business requirements are met even though these might have changed since the original design.
------------	---

verification	An activity that ensures that a solution (or part of) is complete, accurate, reliable and matches its design specification.
--------------	---

