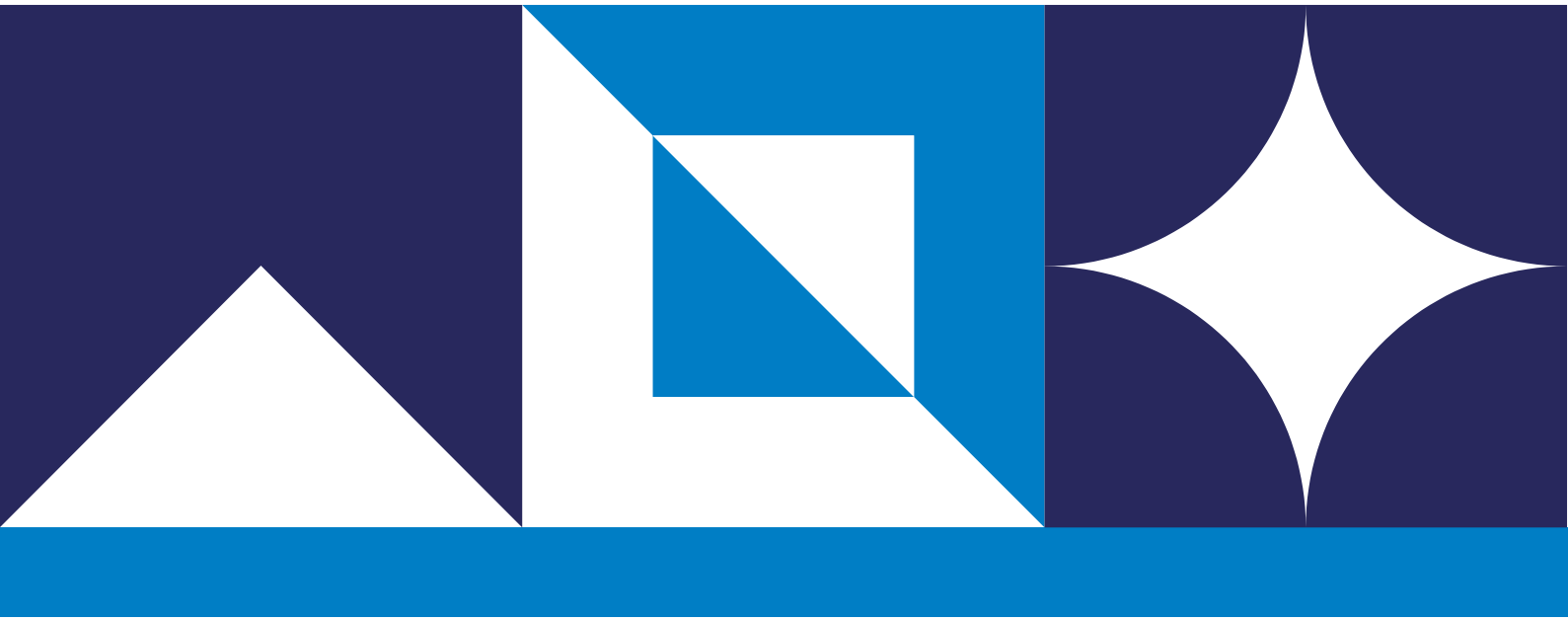
HM Government

Government Functional Standard



GovS 005: Digital

Version: 2.1
Date issued: December 2023

Approved

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 2.1 of GovS005 replaces version 2.0. Minor update, changing references to the function from the Digital, Data and Technology function to Government Digital and Data function, reflecting new branding. No changes or additions to requirements and recommendations.

Version 2.0 of GovS 005 replaces version 1.0 and has the same purpose, scope and intent. The main changes relate to general enhancements derived from use, feedback and changes to other standards. The promotion of the below have been reflected in the document:

- the use of digital approaches and cross-functional teams in policy design and delivery
- product-centric organisational structures and agile ways of working
- digital transformation as a priority
- organisations having a clear view and owner of the services they deliver
- digital, data and technology being represented at a senior level in organisations

Produced by the Government Digital and Data function

Contents

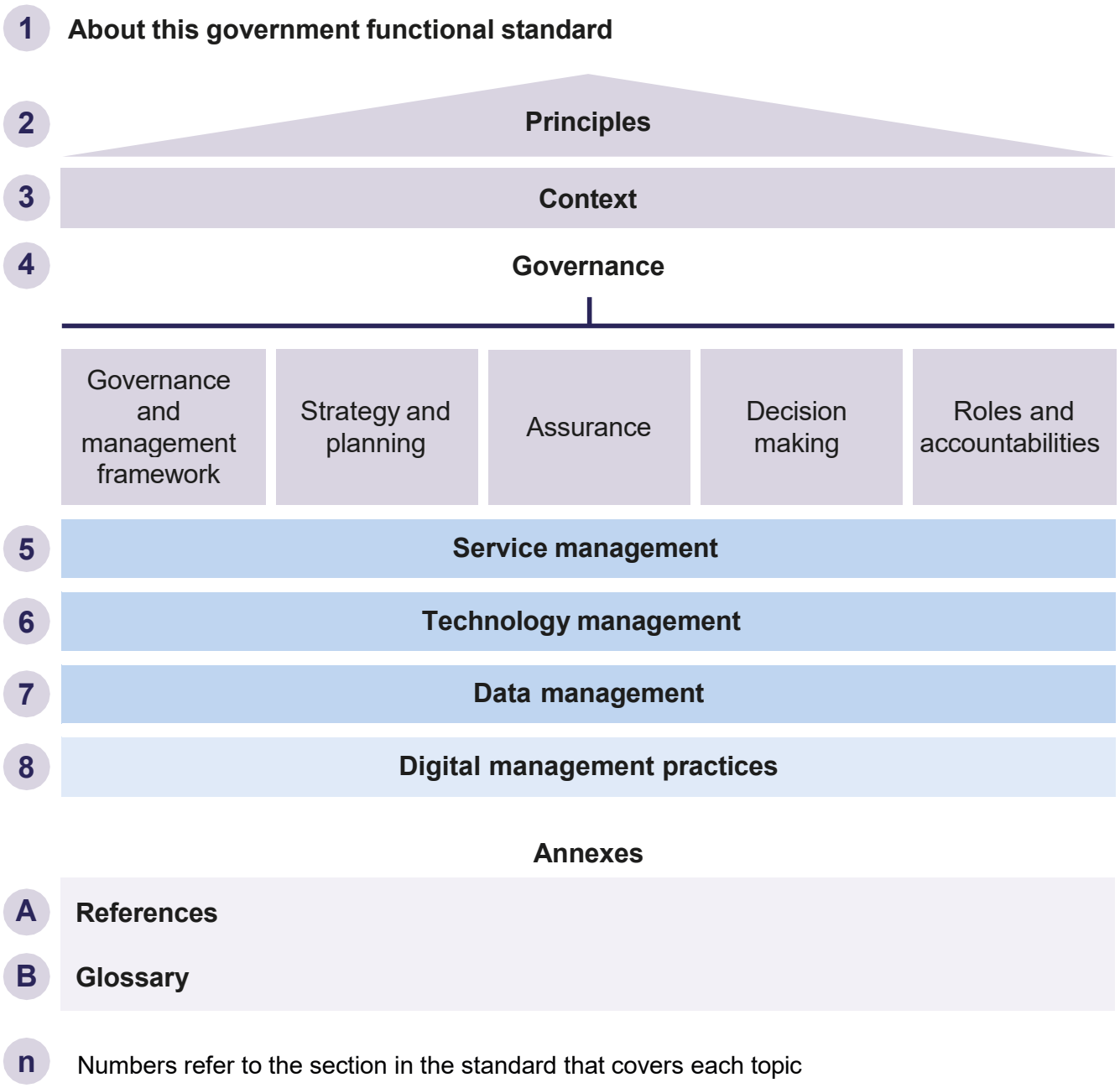


Figure 1 Structure and scope of this standard

1. About this government functional standard

1.1 Purpose of this standard

The purpose of this government functional standard is to set expectations for the management of digital, data and technology in government in order to:

- enable defined policy outcomes
- improve the usability and efficiency of government services
- improve the operating effectiveness of government organisations

This standard provides direction and guidance for:

- permanent secretaries, directors general, chief executive officers of arm's length bodies and third-party suppliers
- senior officers accountable for digital, data and technology across government and in organisations
- senior officers responsible for strategy, policy and delivery
- practitioners involved in planning, developing, delivering or managing digital, data and technology related activity

1.2 Scope of this standard

This functional standard applies to the planning, development, delivery and management of:

- services, including both digital and non-digital elements
- technology
- data

This standard applies to internal and public-facing digital, data and technology activity in government departments and their arm's length bodies.

While all digital products and services should be designed for security, the management of cyber security is outside the scope of this standard (see GovS 007, Security).

Other public sector organisations, devolved or local, may adopt this standard in full, or use it to support benchmarking and continuous improvement. Where use of the standard is limited to benchmarking and continuous improvement, mandatory elements in the standard may be treated as advisory.

Note: An organisation, in the context of government functional standards, is the generic term used to describe a government department, arm's length body, or any other entity that is identified as being within scope of a functional standard.

The structure of the standard is shown in Figure 1.

1.3 Government standards references

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

A functional standard supports achievement of the outcomes sought by an organisation. It sets expectations for what needs to be done and why relating to the functional work within its scope, in order to achieve those organisational outcomes.

Note: For expectations relating to management of a function across government, and management of functional standards, see GovS 001, Government functions.

2. Principles

Those engaged in the planning, development, delivery and management of digital, data and technology shall ensure:

1. activity aligns to government policy and organisational objectives
2. governance and management frameworks are proportionate and appropriate to the work and the level of prevailing risk
3. accountabilities and responsibilities are defined, mutually consistent, and traceable across all levels of management
4. services are built around user needs and business outcomes, which are continuously assessed, measured and validated throughout the service life cycle
5. services are delivered by multi-disciplinary teams, spanning policy, the required technical specialisms and delivery, with the required capability and capacity
6. services are managed to avoid and actively reduce the proliferation of legacy systems and outdated technology
7. technology is designed to be made available to share and reuse across organisations and functions, where appropriate
8. data is collected, stored, shared and used in an appropriate and ethical way
9. public service codes of conduct and ethics, and those of associated professions, are upheld

3. Context

3.1 Introduction

This section provides essential background information for the use of this functional standard.

3.2 Digital transformation

Digital transformation involves the end-to-end transformation of services through redesigning existing business processes in order to make them usable and efficient. It also involves the modernisation of underpinning technology and more effective access to and use of data.

Product-centric delivery involves restructuring organisations around product or service ownership. This means:

- there are single accountable owners for end-to-end products and services
- cross-functional teams work to drive improvements against agreed objectives and measurements

3.3 Services

A service delivers an outcome for users and can result from government policy or user needs.

A service can be public user-focused, such as claiming benefits or applying for a licence, or internal user-focused, such as HR platforms or travel booking.

A service can include digital and non-digital elements, which need to operate together to meet user needs. A digital element of a service is usually enabled through digital channels, for example, online forms. The non-digital elements of a service involve human interaction, for example, face-to-face interactions at a job centre.

3.4 Technology

Technology refers to both hardware and software components.

Hardware components are physical systems (such as computers, storage, networks and other physical devices, and infrastructure) to create, process, store, secure and exchange all forms of electronic data.

Software components comprise applications and other system software (such as operating systems, device drivers and code), which are used to:

- create interfaces for users (for example, a front-end for citizen users, or an interface for those maintaining the technology)
- enable undertaking specific tasks (such as back-office processes)

3.5 Data

Data is used and managed to provide users with consistent information about people, things and systems in ways that are suitable for communication, interpretation or processing.

Types of data include:

- personal data, such as names and contact details
- data about location and environment, such as geospatial reference details
- administrative records about businesses and public services, such as asset lists

Uses for data in government include:

- informing policy design, development and evaluation
- monitoring and reporting (for example, national statistics)

- supporting delivery of a government service (for example, cross-checking data on immigration status to determine an individual's eligibility for benefits)
- understanding and improving organisations' business performance to enable risk-based decision making (for example, the use of predictive analytics)

4. Governance

4.1 Governance and management framework

4.1.1 Overview

Governance comprises prioritising, authorising, empowering, overseeing, and assuring performance. This should be undertaken across government and within each organisation.

A governance and management framework shall be defined and established by those accountable for managing digital, data and technology related activity to ensure governance is effective and structured. It should include:

- delegated authority limits, decision making roles and rules, degrees of autonomy, assurance needs, reporting structure, accountabilities, roles and escalation routes
- the appropriate management practices and associated documentation needed to meet this standard

4.1.2 Governance across government

A senior officer accountable for digital strategy and planning across government shall be assigned (see 4.5.2). They should define the cross-government governance and management framework in consultation with those leading digital, data and technology in organisations (see 4.5.4).

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
- capability requirements
- guidance for practitioners

4.1.3 Governance within each organisation

The governance of digital, data and technology related work within an organisation should be an integrated part of that organisation's overall governance. The governance and management framework should bring together digital and non-digital business leaders to enable digital work to be prioritised.

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)

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

- required strategies and plans (see 4.2)
- a pipeline of proposed, current and completed work, including associated spend

A senior officer accountable for the governance of the organisation's digital, data and technology shall be assigned (see 4.5.4).

4.2 Strategy and planning

4.2.1 Cross-government digital strategy

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

- synergy, efficiency, and interoperability of digital, data and technology related activity and assets within and among organisations
- significant programmes
- the organisation's targets and targets for digital, data and technology being met
- capability and capacity requirements
- how the strategy is to be implemented

The cross-government digital strategy shall be developed in collaboration with senior business leaders and digital specialists across government. It shall be communicated to organisations and used to support decision making (see 4.4).

Note: For the cross-government digital strategy, see Transforming for a Digital Future [1].

Note: For data and information, see the National Data Strategy [2].

4.2.2 Digital strategy and planning in an organisation

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

- align to the cross-government digital strategy (see 4.2.1)
- align to the organisation's policy and strategy
- be subject to approval by the accounting officer (see 4.5.3)

The digital strategy should be developed collaboratively by the organisation's senior leaders and led by the senior officer accountable for the organisation's digital portfolio (see 4.5.4). It should reach at least three to five years into the future, and should:

- outline the organisation's ambition for how digital, data and technology is to 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 is to achieve its objective for each of digital, data, technology and capability

The digital strategy should be endorsed and actively supported by the accounting officer (see 4.5.3) and senior leadership as this is critical to achieving digital transformation.

A detailed plan for digital, data and technology related activity setting out owners, milestones and key performance indicators should be drafted, agreed with relevant senior leaders, and reported against quarterly.

4.3 Assurance

The purpose of assurance is to provide confidence to senior leaders and stakeholders that work is controlled and supports efficient and successful delivery of policy, strategy and objectives.

Organisations should have a defined and established approach to assurance of digital, data and technology spend and activity, which should be applied proportionately to the risk and value of the activity, and integrated with the organisation's overall assurance framework. Assurance should align to cross-government strategy and standards, including centrally provided requirements mandating specific assurance activities.

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.

GovS 009, Internal audit shall be complied with.

The requirements of the Orange Book: management of risk - principles and concepts, shall be met [31].

4.4 Decision making

Decisions relating to digital, data and technology activity should be made, and approvals and authorisation given, in a timely manner, in accordance with the organisation's governance and management framework. Where specified, minimum expectations shall be met (see 4.2.1).

Decisions should be made by assessing options against defined criteria and in consultation with stakeholders and subject matter experts.

Key decisions, relating to digital, data and technology activity should include:

- alignment to cross-government and organisational strategy and plans
- authorising programmes and projects (see GovS 002, Project delivery)
- efficiency and value
- sustainability of options, including the purchase of products and services (see GovS 008, Commercial)

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

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).

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

GovS 010, Analysis shall be complied with, with respect to the assessment of options.

Organisations shall comply with expenditure controls guidance [3].

Organisations shall comply with guidance on how to handle public funds [34].

4.5 Roles and accountabilities

4.5.1 Overview

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

This should include, but is not limited to, the activities, outputs or outcomes they are responsible for, and the person they are accountable to.

4.5.2 Senior officer accountable for digital strategy and planning across government

The senior officer accountable for digital strategy and planning across government is accountable to the Chief Operating Officer of the government for:

- providing leadership and direction for digital transformation and policy across government (see 3.2)
- setting and maintaining the cross-government governance and management framework (see 4.1)
- defining, communicating and implementing the cross-government digital strategy, policy and plans (see 4.2.1)
- continuous improvement in the government's use of technology and data to support improved services (see sections 5, 6, 7) and digital practices (see section 8)

Note: This role is done by the Government Chief Digital Officer in the Central Digital and Data Office, who also leads the Government Digital and Data function across government.

4.5.3 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 digital strategy is appropriate (see 4.2.2), and should create an environment in which their organisation:

- endorses and actively supports digital transformation
- plans and manages digital, data and technology related activity in accordance with this standard

4.5.4 Senior officer accountable for an organisation's digital portfolio

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

- providing leadership and direction for digital 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 digital strategy and plans (see 4.2)

- ensuring continuous improvement of digital, data and technology related 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 4.5.7)
- managing digital, data and technology related risk within the organisation's risk appetite and tolerance (see 8.12)

The senior officer accountable for an organisation's digital portfolio should be a member of the organisation's senior decision making forums to ensure that the organisation's digital strategy needs are represented.

Note: In the majority of organisations this role is a Director or Director General.

Note: This role is often known as Chief Digital Officer, who in most cases would also lead the organisation's Government Digital and Data function.

Note: See GovS 002, Project delivery for more on portfolio, programme or project management.

4.5.5 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 digital portfolio (4.5.4), for managing the organisation's data (see section 7) in relation to digital 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

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.

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 GovS 010, Analysis.

4.5.6 Senior officer accountable for technology in an organisation

The senior officer accountable for technology in an organisation is accountable to the senior officer accountable for the organisation's digital portfolio (see 4.5.4), for managing the organisation's technology (see section 6), and for ensuring that the organisation:

- adopts and complies with relevant technology requirements and guidance (see 4.1)
- develops, maintains and implements a technology strategy and plan (see 4.2)

- assigns appropriate roles and responsibilities for the ownership and management of technology
- has an appropriate approach to technical security and resilience

This role should provide technical direction for the design and delivery of services (see section 5), so that the organisation uses technology in an appropriate, cost-effective, scalable way, while maintaining the operational sustainability and resilience of the services.

See section 6, Technology 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.

4.5.7 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
- the organisation uses performance data and user feedback to understand how well services are performing in terms of usability and efficiency
- accountabilities and responsibilities for each service are assigned, with service owners taking end-to-end responsibility (see 4.5.8)
- appropriate provision is made for users who are not using digital channels

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.

4.5.8 Service owner

The service owner is accountable to the senior officer accountable for service delivery (4.5.7) 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 8.12)
- 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 4.5.9) 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 in digital channels).

4.5.9 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 8.12)
- delivering continuous improvements, enhancements and updates

5. Service management

5.1 Overview

The purpose of this section is to provide a framework for development, management, improvement and, where needed, retirement of a service.

Services should be delivered digitally, where possible, and that delivery should be developed and delivered through multi-disciplinary teams using agile management techniques and frameworks.

Accountability for the ownership and management of service delivery and each service shall be assigned (see 4.5.7 and 4.5.8).

5.2 Policy intent

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

The outcomes, efficiencies and benefits of a service should be defined so that they are traceable to the achievement of, or support for, defined policy intent.

Policy owners and those accountable for service delivery should work together in cross-functional teams under a single service owner to ensure policy intent is reflected on a continuous basis.

5.3 Service design and development

New services and services undergoing change and transformation should provide value to both government and to users, and be usable and efficient. See GovS 002, Project delivery.

Services shall be delivered in accordance with the Service Standard [32] through all phases of the service life cycle.

User research (see 8.3) and iterative development should be undertaken throughout the service life cycle to ensure continuous improvement. Services shall be monitored using consistent measures of service performance (see 5.6), which should be reviewed quarterly.

Where services are not yet delivered digitally, or are performing poorly against usability and efficiency measures, the service owner should consider the need to redesign the service end-to-end.

Organisations that choose to buy off-the-shelf products and services should ensure that suppliers are able to meet the needs of service users. See 6.3 and GovS 008, Commercial.

GovS 007, Security shall be complied with, with respect to embedding cyber security into a digital service throughout its life cycle.

Note: Advice and guidance about technology choices can be found in the Technology Code of Practice [7].

Note: The Service Manual [8] includes advice on creating and running public services that meet the Service Standard.

5.4 Service management

Services should be documented so that its architecture, components and the connections between them 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

A target operating model for each service should be developed and maintained. The model should set out the delivery approach (see 8.2), working practices and processes, people and skills, data and technology needed to provide the service.

Integrated management should be put in place among:

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

Services should be delivered and improved iteratively to meet the changing needs of their users, changes in technology and government policy, releasing value via frequent deployment cycles.

Service owners and their teams should use qualitative and quantitative data, for example, performance analytics (see 5.6), user feedback and user research (see 8.3) to inform and prioritise how to iteratively deliver and improve their service. Such 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 to ensure all public and internal facing digital services and internal technologies are discoverable for use, and possible reuse, across the organisation and other organisations.

The portfolio of services should be maintained to ensure:

- technology, data and non-digital components of services are planned and managed as part of a unified and consistent system

- 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 guidance set in the cross-government performance framework.

Targets for performance of the service should be established and managed. These should align to cross-government performance metrics and should include:

- data on useability and efficiency of the service
- meeting defined service levels

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

5.7 Accessible and inclusive services

Making services accessible and inclusive means ensuring that any potential user is able to use the service regardless of their personal characteristics, situation, capabilities or access needs, and is given equal access and opportunity to do so.

Digital services shall be designed and managed to meet the needs of users with defined ranges of abilities, or defined accessibility requirements. Relevant legislation shall be identified and must be complied with.

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, but provide help (including non-digital alternatives) for those who don't have 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 [8].

Note: The Service Standard [32] sets requirements for accessibility, useability, consistency and efficiency.

Note: Attention is drawn to the public sector accessibility regulations [4].

5.8 Service retirement

The senior officer accountable for the organisation's service delivery (see 4.5.7) may decide to retire the service, taking advice from the service owner. The decision might relate to, for example, changes in policy or user need, or to consolidate with another service.

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
- ensure impacted stakeholders are engaged

6. Technology management

6.1 Overview

A senior officer accountable for technology in each organisation shall be assigned (see 4.5.6).

The senior officer accountable for technology in an organisation should incorporate insights and research into the organisation's strategy, technology architecture and asset management strategy (see 8.8).

GovS 002, Project delivery shall be complied with, with respect to work that is part of a portfolio, programme or project.

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

- The Technology Code of Practice [7]
- Cloud First Strategy [9]
- Managing Vendor Lock-in [10]
- National Institute of Standards and Technology [11]
- Cyber Essentials [12] (and other levels of security assurance as required)

6.2 Technology development and maintenance

Technology architecture sets parameters for the efficient configuration, interaction and interdependence of the components (or configuration items) of a technology solution or system.

The technology architecture should be aligned to the target operating model for a relevant service or services and data requirements (see 5.4 and 8.4).

Technology architecture should reflect the organisation's technology strategy, support existing and future delivery of the organisation's services, and be deliverable within the organisation's risk appetite (see 8.12).

In keeping with the published standards (see 6.1), technology should:

- be secure by design
- use open standards and open code
- adhere to its classification standards
- protect its data, at rest and in transit

Technology used within and by an organisation should be understood and managed, with suitable governance controls in place to reduce or remove legacy technology, manage technical debt, track alignment with other organisations and understand vendor usage and supply chain. The aim should be to reduce the scope and spread of new technologies to ensure efficient and effective solutions across government. Governance controls should consider a full understanding of the business continuity and resilience of a solution.

Organisations should be aware of and manage its risks and dependencies in a clear and documented way, ensuring a regular review of external dependencies, including supply chain, especially where sharing is in place (see 8.12).

Technology solutions may be developed and managed in-house or by third-party suppliers (see 8.12).

6.3 Deployment and operation of technology

6.3.1 Overview

Each organisation should have mechanisms in place for managing and continually improving its technology solutions, so that changing requirements are identified, and business and user needs continue to be met.

Relevant roles and responsibilities should be defined and assigned to reflect the build or buy (see 8.12) choices taken by the organisation.

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 [7].

6.3.2 Operations management

The senior officer accountable for technology in the organisation (see 4.5.6) should ensure that those managing operation of the technology have the capability and capacity to do so, and have defined processes to run, operate, and continuously improve the technology solution.

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, effective operational monitoring, including the full range of Information Technology Infrastructure Library (ITIL) 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

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 the technology, including user feedback 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 technology architecture (see 6.2)

Addressing the triggers for change might result in incremental change or upgrades managed as a project or programme.

The organisation's legacy technology should be defined and monitored. An up-to-date plan should be maintained to either remediate or retire the legacy technology.

Technology becomes legacy when it is any or all of the following points:

- 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

6.4 Technology retirement

6.4.1 Overview

The purpose of technology retirement is to ensure that technology remains fit for purpose. Technology should be considered for retirement if:

- it is not possible to update or improve existing technology to meet future business or user needs
- there are resource constraints
- the technology 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 technology strategy

The senior officer accountable for technology in an organisation (see 4.5.6) should:

- identify technology components that are no longer capable of meeting the organisation's needs
- identify the services or business operations that rely on the technology intended for retirement
- consult service owners and other stakeholders that rely on the existing technology, to understand their priorities for the future operation
- oversee service delivery teams to ensure the management and retirement of technology and, where necessary, its replacement, meets the organisation's needs
- work with the service owners and stakeholders to ensure all data is appropriately dealt with either through migration, archiving or removal based on the GDPR and classification and information assurance requirements of the solution
- lead the removal and appropriate disposal of the retired technologies

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

Note: Retire includes withdrawal from existing services or operations, and disposal of the technology assets.

6.4.2 Withdraw technology

The process and complexity of moving away from legacy systems and technologies varies depending on the technology 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 technology 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 technologies, 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
- engage with staff and other users affected by the change, and provide necessary training or guidance

6.4.3 Dispose of technology

The service owner (see 4.5.8) and the senior officer accountable for technology in an organisation (see 4.5.6) should ensure redundant equipment is 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, processes should be followed to ensure residual data is not accessible post-disposal. The relevant security cluster or National Cyber Security Centre guidance should always be considered when disposing of technology.

Requirements for the proper handling of personal data being moved or removed must be followed in accordance with prevailing regulations and other security advice.

Note: Attention is drawn to:

- General Data Protection Regulation [5]
- The Data Protection Act [6]

GovS 007, Security shall be complied with.

7. Data management

7.1 Overview

This section sets expectations for managing and maintaining data to benefit the public and government. Data should be treated as an important corporate asset that supports the organisation's business and service delivery.

A senior officer accountable for data in each organisation shall be assigned (see 4.5.5).

Organisations should follow the expectations set in the cross-government strategy and follow the cross-government governance, including compliance with relevant standards (see section 4).

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

Note: The National Data Strategy [2] sets government's ambition to transform data use in government.

Note: Attention is drawn to:

- General Data Protection Regulation [5]
- The Data Protection Act [6]

7.2 Data management principles

Data management must be legally compliant.

Organisations should ensure their data is fit for purpose through:

- identifying what data is critical in a cross-government data sharing context
- identifying the owner of critical data with accountability for maintaining appropriate levels of data governance and control
- ensuring processes are in place to resolve high priority data quality issues in a timely manner

Organisations should ensure their data is trusted by the users and available through:

- being able to evidence that designated critical data meets minimum standards of governance and control based on the purpose and context of its consumption
- ensuring structures are in place to search for, curate and provision critical data efficiently, subject to appropriate security and access controls

Organisations should ensure their data architecture (see 7.3) is interoperable through:

- being able to identify the authoritative sources of critical data and that it is appropriately sourced, maintained and provisioned
- being able to evidence that application programming interfaces (APIs) and data exchange platforms meet minimum standards of data governance and control so that data is not inadvertently misused or fraudulently exploited (see GovS 013, Counter fraud)
- ensuring that data classifications (criticality, security etc.) are documented to ensure appropriate adherence to frameworks and operating models
- ensuring that there are integrated catalogues for data, interfaces and standards to facilitate data sharing via suitable maintained authoritative sources

There should be appropriate accountable ownership for all aspects of data quality, protection, security and ethics, using the cross-government guidance, frameworks and standards.

In order to promote a culture of continuous improvement and enable senior leaders to focus resources on priority areas, organisations should be regularly assessed against technical, structural and cultural factors to determine their data maturity within a set framework.

Throughout the planning, implementation, and evaluation of a new project or programme, organisations should use the Data Ethics Framework [16] to ensure data is used appropriately and responsibly. See 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 [14], which provides the framework to ensure that statistics are trustworthy, good quality, and valuable. These principles are relevant in many areas of data management and the code should be followed where appropriate.

Note: The Data Standards Authority [15] exists to improve how the public sector manages data, including by setting standards for sharing and using data across government.

Note: The government published a Data Ethics Framework [16], which guides appropriate and responsible data use in government and the wider public sector. It helps public servants understand ethical considerations, address these within their projects, and encourages responsible innovation.

7.3 Data frameworks and operating models

Organisations shall follow appropriate guidance for implementation of frameworks and operating models to ensure appropriate and transparent use of data, including data subject to cross government sharing for business intelligence, artificial intelligence and advanced analytics.

Note: The following products provide best practice guidance:

- Creating and Sharing Spreadsheets Guidance [27]
- The National AI Strategy [28]
- The Algorithmic Transparency Recording Standard [29] helps organisations provide clear information about the algorithmic tools they use, and why they're using them

7.4 Data architecture

Data architecture describes the organisation's systems, processes and structures that manage how data is acquired, transported, stored, queried, and secured to meet business needs.

Organisations rely on data to inform decision making and underpin service delivery, so need confidence that the right data is available where and when it is needed, in usable and standardised formats and systems, and that business needs are met by the appropriate data and system capabilities.

When developing data architecture proposals, relevant standards, guidance and tools should be followed. Data assets should be managed appropriately (see 8.8).

Note: For practical advice, see the data management capability framework [17] and the GOV.UK collection of design guidance for application programming interfaces. 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 [18]
- GraphQL Guidance [19] - an API specification originally developed by Facebook as an alternative to REST for querying complex data structures
- API Management Guidance [20] - enabling you to standardise how teams design, launch and manage APIs in your organisation
- Domain Guidance for api.gov.uk [21] - contact the Government Digital Service to get a domain for your API on GOV.UK

7.4.1 Managing data quality

Data quality should be measured on completeness, uniqueness, consistency, timeliness, validity and accuracy. Different data uses might need different combinations of these depending on context.

Organisations should develop a culture of data quality, by:

- treating issues at source, and committing to ongoing monitoring and reporting
- targeting improvements where they add most value
- managing data quality proactively

A data quality plan may be used to define and manage the organisation's work on data quality improvement. If used, the quality plan 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:

there is accountability (see 4.5.5)

- 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 [22] provides information and support on data quality.

Note: Further information and guidance can be found in the Data Quality Framework [23].

7.5 Data asset management

Data asset management enables an organisation to establish and maintain the knowledge of its data so that it knows where it is, can rely upon its accuracy, can obtain it when and where it is needed, and it is treated as a corporate asset.

Organisations should follow existing standards and should manage data so that:

- data is used multiple times, to maximise value and minimise duplication
- data is available for sharing, unless there are valid reasons not to
- dataset linkage is promoted
- data is easily retrievable
- access permissions are strictly managed
- data governance and compliance for the regulations relevant to the assets are observed
- there is an interoperable data infrastructure
- there are integrated catalogues for data and interfaces
- open standards are used
- cyber security policies are in place
- metadata is actively managed

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

- API Catalogue [24]
- Reference Data for Use Across Government [25]
- Address Base Guidance [26] - use free property and street information to add geospatial data to your projects and comply with the UPRN standard

7.6 Data engineering

The purpose of data engineering is to make data more useful and accessible to a wide variety of customers, so they can make informed data driven decisions and optimise the performance of their organisation.

Data engineering comprises taking raw data, transforming it and storing it in formats appropriate to the users' needs, so that the right data is provided at the right time, in the right format.

In order to ensure useful and accessible data through data engineering, organisations should:

- follow cross-government data standards
- produce, maintain and update relevant data models for specific needs
- have appropriate metadata repositories, and governance in place to manage them
- ensure there are data integration procedures across the data development life cycle

8. Digital management practices

8.1 Overview

The digital management practices in this section support development, delivery and ongoing monitoring of appropriate and sustainable digital, data and technology related activity. They apply across the scope of this standard.

Managers of digital, data and technology related activity, supported, where necessary, by subject matter experts, should plan, manage and monitor the work so that:

- there is a defined and established delivery approach (see 8.2)
- policy and business outcomes are met through user-centred design (see 8.3)
- digital components are integrated or interoperable where appropriate (see 8.4)
- information and knowledge is managed appropriately (see 8.5)
- channel strategies and customer relations are managed appropriately (see 8.6)
- sustainability is considered throughout the life cycle of a product or service (see 8.7)
- assets are managed appropriately (see 8.8)
- performance is managed consistently (see 8.9)
- management information is provided in an accurate, complete and timely manner (see 8.10)
- there is the required digital capacity and capability (see 8.11)
- associated risks are identified and managed (see 8.12)
- externally sourced products and services are managed appropriately (see 8.13)

8.2 Delivery approach

8.2.1 Choose the right delivery approach

A delivery approach sets out how a solution is to be delivered, implemented, managed and decommissioned. For most digital, data and technology activity, the default approach should be agile (see 8.2.2), delivered through a product-centric approach.

The person leading the work (for a service, this is the service owner, see 4.5.8) should define and establish an appropriate delivery approach to their assigned problem. The approach should:

- include mechanisms to assure the quality and control of the work (see 4.3)
- adhere to relevant cross-government standards, guidance and requirements (see 4.1.2)
- consider where skills are required and sourced

The delivery approach should be chosen to take into account:

- whether the work is a new solution, or enhancement to an existing product or service
- confidence in user needs and business requirements
- the required timescales
- the type of outputs required and whether user value can be delivered incrementally
- the risk associated with the development, verification, validation and deployment of each element of the solution (see 8.12)

Different delivery approaches may be used for different components of a wider system (whether managed as a service, programme or project), but should be defined so that components:

- can be integrated at appropriate points in the design, development and delivery of the system
- are managed within the overall risk associated with the system
- follow relevant digital, data and technology architectures

The use of agile techniques and behaviours and the incremental release of minimally viable products that deliver value to users in the short term should be considered when defining the delivery approach that should be taken.

Services (see section 5) shall be delivered in accordance with the Service Standard [32].

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 delivery approaches should be used where rapid value creation and flexibility are needed and shall be routinely adopted for digital, data and technology, unless predictive delivery is necessary (see 8.2.3).

Agile culture and behaviours, such as multi-disciplinary teams, that enable delivery teams to continuously improve their user-centred services whilst meeting delivery milestones should be promoted.

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

See GovS 002, Project delivery.

8.2.3 Predictive delivery approaches

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

Examples of where non-agile delivery approaches are likely to be appropriate include:

- large capital infrastructure projects, such as large-scale transport projects, where it is impossible to release value incrementally
- complex infrastructure remediation programmes where there is limited benefit to introducing greater uncertainty into the delivery process
- work on tightly coupled (typically legacy) systems where significant system dependencies limit the ability to rapidly iterate
- work on safety critical systems where a test and learn approach would introduce substantial and unmitigable 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

The purpose of user-centred design is to ensure that a digital solution meets the current and future needs of users in an accessible, inclusive (see 5.7) and timely way, and is in line with policy and business objectives (see 5.2).

Note: Attention is drawn to the public sector accessibility regulations [4].

User-centred design is a collection of practices that should be followed to ensure that user needs are:

- clearly identified, understood and used to inform service design and set objectives
- balanced with the outcomes that government wants to achieve

User needs should be used to design a digital solution that is efficient and enables users to achieve their goals more easily than current practices.

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

Re-use of technology and a focus on interoperability reduces duplication, saves money and enables a more coherent and consistent user experience.

Organisations should develop and maintain required catalogues for services, data and technology.

Catalogues should include public-facing and internal information, such that their content is discoverable for use, and possible reuse, across the organisation and in other government organisations.

8.5 Information and knowledge management

Information and knowledge management ensures information and knowledge is available and reliable for undertaking work and making decisions.

The organisation’s information requirements should be understood and documented.

Critical information should be identified in the data and information part of the organisation's digital strategy, and reflected in the organisation's plans (see 4.2.2) and asset management arrangements (see 8.8).

The status, security classification and provenance of information and data should be clear. Information should be retained to meet statutory, contractual and wider business requirements.

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.

When considering channels for the organisation's portfolio of services, and for each service, organisations should understand:

- current channel usage patterns and associated costs
- how users transition from one channel to another
- which channels are needed by which user groups
- what remediation is in place if a failure by one channel puts additional pressure on other channels
- how a service is to be made accessible and inclusive (see 5.7)

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, in order to reduce demand for updates.

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

8.7 Sustainability

Sustainability is concerned with meeting present needs without compromising the environment for future generations. In relation to digital, data and technology, all digital solutions (including services) shall be designed with sustainability in mind.

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.

Where possible, waste should be removed from the system, such as redundant services, duplicate files, legacy technology systems and hardware, promoting shared systems and services across government.

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 sustainable ICT and digital services strategy [33] for more on delivering sustainable digital solutions.

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 strategies (see 4.2).

Asset management plans should be developed and maintained to support configuration across the organisation's digital portfolio. This should cover elements including:

- 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 the technology 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 to establish and 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 original copy of data as it is received
- ensure data is backed up
- ensure data has metadata
- keep an audit trail of changes throughout the life cycle of data
- ensure data can be rolled-back to its 'as-received' state
- actively manage, review and improve 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 to cross-government performance frameworks in order to enable consistent measurement and reporting of service performance, technology estate and digital maturity.

8.10 Management information, analytics and reporting

Management information should be provided in an accurate, complete and timely manner to ensure those relying on it can undertake their roles effectively.

System workflows and real-time dashboards should be used to ensure processes and transactions are progressing.

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 capacity and capability management balances the supply and demand for appropriate resources, such as skilled people, equipment, material and facilities, to be deployed when needed. Resources can be sourced from within government, by recruitment or from the supply chain.

A comprehensive view of current and future skills needs should be developed and maintained, with possible shortfalls identified and addressed. Capacity should be developed and managed to meet the planned needs. If insufficient resources are available, work should be re-planned to reflect such constraints. Business continuity measures should be in place in the event of the loss of critical resources. Where better value can be derived from using third parties to deliver products and services, this resourcing route should be used in accordance with the Digital, Data and Technology Playbook [35]. Organisations should capture the use of third parties and associated skill deployment on work in their capacity and capability plans.

Senior civil servants within an organisation shall be assessed against the Digital and Data Essentials standard [30].

GovS 003, Human resources shall be complied with, with respect to people management.

8.12 Risk management

The purpose of risk management is to ensure digital solutions operate successfully in support of objectives, taking into account the extent of identified threats and opportunities.

The senior officer accountable for the organisation's digital portfolio (see 4.5.4) 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

The risks associated with digital, data and technology related activity should be represented at board level in organisations, and time should be given to regularly review and understand these risks in relation to sustainability of investment, continual improvement, capability, security and management of legacy and technical debt.

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 [31].

8.13 Purchasing and contract management

8.13.1 Procurement

Organisations shall identify and decide whether service solutions or components should be built and managed by the organisation, supplied and managed by a third party, or delivered through a combination of both approaches.

To support these build or buy decisions, each organisation should define and maintain a purchasing strategy, to support consideration of commercial, contractual and technology aspects.

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 a new solution or investment to tailor an existing solution should only be considered where:

- user need is unique or rare
- there are limited suppliers available
- commercial products cannot be scaled or adapted to meet the need
- there are specific reasons for an organisation to own and modify the technology

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.

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

Note: See Should Cost modelling for purchasing strategy guidance [13].

8.13.2 Contract management

A contract management plan should be established that defines the roles and the responsibilities of each party, and should be reviewed periodically throughout the life of the contract.

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
	Government references
1	Central Digital and Data Office, *Transforming for a digital future* (2022)
2	Department for Digital, Culture, Media and Sport, *National Data Strategy* (2020)
3	Central Digital and Data Office, *Cabinet Office Controls* (2021)
4	Central Digital and Data Office, *Understanding accessibility requirements for public sector bodies* (2022)
7	Central Digital and Data Office, *The Technology Code of Practice* (2021)
8	*Service Manual*
9	Central Digital and Data Office, *Government Cloud First policy* (2022)
10	Central Digital and Data Office, *Managing technical lock-in in the cloud* (2019)
12	National Cyber Security Centre, *Cyber Essentials*
13	Government Commercial Function, *Should Cost Modelling* (2021)
15	*Data Standards Authority*
16	Central Digital and Data Office, *Data Ethics Framework* (2020)
17	Central Digital and Data Office, Government *Digital and Data Profession Capability Framework* (2022)
18	Central Digital and Data Office, *Develop your data and APIs using a reference architecture* (2021)
19	Central Digital and Data Office, *Using GraphQL for your API* (2021)
20	Central Digital and Data Office, *Defining an API management strategy* (2021)
21	Central Digital and Data Office, *Get an API domain on GOV.UK* (2021)
22	Office for National Statistics, *Government Data Quality Hub*
23	Government Data Quality Hub, *The Government Data Quality Framework* (2020)
24	Central Digital and Data Office, *UK public sector APIs*

ID	Description
	Government references
25	Central Digital and Data Office, *Publish reference data for use across government* (2021)
26	Central Digital and Data Office, *Access free address data using AddressBase* (2021)
27	Central Digital and Data Office, *Creating and sharing spreadsheets* (2021)
28	Office for Artificial Intelligence, Department for Digital, Culture, Media & Sport, and Department for Business, Energy & Industrial Strategy, *National AI Strategy* (2022)
29	Central Digital and Data Office, *Algorithmic Transparency Reports* (2023)
30	Central Digital and Data Office, *Digital and Data essentials for senior civil servants* (2022)
31	HM Treasury, Orange Book: *Management of risk - Principles and Concepts* (2021)
32	*Service Standard*
33	Department for Environment, Food and Rural Affairs *Sustainable ICT and digital services strategy* (2020)
34	HM Treasury, *Managing Public Money* (2022)
35	Digital, Data and Technology Profession, *The Digital, Data and Technology Playbook* (2022)
	External references
5	*General Data Protection Regulation*
6	*Data Protection Act*
11	*National Institute of Standards and Technology*
14	*Code of Practice for Statistics* (2022)

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
agile	An umbrella term for a collection of frameworks and techniques that together enable teams and individuals to work in a way that is typified by collaboration, prioritisation, iterative and incremental delivery, and timeboxing. Note: There are many specific methods (or frameworks) that are classed as Agile, such as Scrum, Lean, and Kanban.
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.
assurance	A general term for the confidence that can be derived from objective information over the successful conduct of activities, the efficient and effective design and operation of internal control, compliance with internal and external requirements, and the production of insightful and credible information to support decision making. Confidence diminishes when there are uncertainties around the integrity of information or of underlying processes.
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).

Term	Definition
configuration	An arrangement of configuration items or other resources that work together to deliver a product or service. Note: Used to determine two-way traceability. Note: Can also be used to describe the parameter settings for one or more configuration items.
configuration item	A component that needs to be managed in order to deliver a service.
data	Information that has been translated into a form that is efficient for movement or processing.
defined (way of working)	In the context of standards, 'defined' denotes a documented way of working which people are expected to use. This can apply to any aspect of a governance or management framework, for example, processes, codes of practice, methods, templates, tools and guides.
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.
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.
established (way of working)	In the context of standards, 'established' denotes a way of working that is implemented and used throughout the organisation. This can apply to any aspect of a governance or management framework, for example, processes, codes of practice, methods, templates, tools and guides.
event (digital)	A change of state that has significance for the management of a service or other configuration item.

Term	Definition
governance	Governance defines relationships and the distribution of rights and responsibilities among those who work with and in the organisation. It determines the rules and procedures through which the organisational objectives are set, and provides the means of attaining those objectives and monitoring performance. Importantly, it defines where accountability lies throughout the organisation.
governance and management framework	A governance and management framework sets out the authority limits, decision making roles and rules, degrees of autonomy, assurance needs, reporting structure, accountabilities and roles and the appropriate management practices and associated documentation needed to meet this standard.
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.
legacy (digital)	A service or component part of a service which is no longer considered fit for purpose.
life cycle	Phased evolution of a system, product, service, project or other human-made entity from conception through to closure or retirement. Note: Examples include service life cycle, system life cycle, data life cycle, project life cycle, programme life cycle.
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.
organisation	An organisation, in the context of government functional standards, is the generic term used to describe a government department, arm's length body, or any other entity that is identified as being within scope of a functional standard.
plan	A plan ensures that desired outputs and outcomes are likely to be delivered within defined constraints, to meet an agreed strategy.
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.

Term	Definition
portfolio	A portfolio comprises part or all of an organisation's investment required to achieve its objectives. Governed through its portfolios (or business) plan, a portfolio comprises work components, such as other portfolios, programmes, projects, other related work and work packages.
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 of time 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.
risk	The effect of uncertainty on objectives. Note: Risk is usually expressed in terms of causes, potential events, and their consequences: • a cause is an element which alone or in combination has the potential to give rise to risk • an event is an occurrence or change of a set of circumstances and can be something that is expected which does not happen or something that is not expected which does happen. Events can have multiple causes and consequences and can affect multiple objectives • the consequences should the event happen – consequences are the outcome of an event affecting objectives, which can be certain or uncertain, can have positive or negative direct of indirect effects on objectives, can be expressed qualitatively or quantitatively
roadmap	A high-level document that outlines what your organisation or team wants to achieve, identifying some initiatives that can help you get there.

Term	Definition
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.
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 backlog	A list of new features, changes to existing features, bug fixes, infrastructure changes or other activities that a team may deliver in order 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.
strategy	A strategy outlines longer term objectives, outcomes and outputs, and the means to achieve them, to inform future decisions and planning.
system	A collection of different components that work together to produce better results than if the component parts were working independently. Note: A system is sometimes considered as a product, or as the services it provides. Note: A complete system includes all of the associated equipment, facilities, material, computer programs, firmware, technical documentation, services and personnel required for operations and support to the degree necessary for self-sufficient use in its intended environment. Note: In practice, the interpretation of a system's meaning is often clarified by the use of an associative noun such as 'aircraft system'.
system of systems	A collection of systems that work together to produce better results than if the component systems were working independently. Note: Component systems fulfil a purpose of their own, and can operate without being part of the system of systems.

Term	Definition
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.
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.

Term	Definition
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.