The National Archives

Business requirements for managing digital information and records

This publication is available for download at nationalarchives.gov.uk.

Contents

Introduction

This guidance describes eight common outcomes that if delivered will ensure the value of digital information, and the benefits of managing it, are realised. Business requirements describe at the highest level what the business should achieve and why. The ways in which they are met through applications and process - the how - are detailed within functional or operational specifications. The business requirements are:

1. user focus.
2. governance, ownership and accountability
3. proportionate use of resources
4. applications perform consistently
5. digital continuity
6. disposal
7. transfer
8. audit and compliance

Individual organisations may have additional requirements which are out of the scope of this guidance.

The National Archives has worked with a number of government departments to develop this common set of outcomes. They support the realisation of the benefits of managing digital information (and records) without adding complex sets of rules or applications that users do not need or cannot apply within their individual context. They support the need for ensuring governance, compliance and standards within an organisation’s strategy to build its digital information management capability. They are flexible and user-focused, promoting the department's management of risk and the understanding and utilisation of existing tools.

The requirements align with the second of the Information principles: ‘information must be managed’, and are themselves further supported by the Section 46 Code of practice and other guidance provided by The National Archives.

The benefits of managing information

The successful management of information is an enabler for:

- the efficient and effective delivery of services to government and to the citizen
- the exploitation, sharing, use and re-use of an organisation's information assets
- the potential rationalisation of an organisation's technology infrastructure
- the efficient and effective use of the technology infrastructure
- transparency, accountability, citizen participation and legislative compliance
- the mitigation of the risk of loss of information within line of business systems and applications

Achieving these outcomes requires a balance between enabling the users' need for information availability (the business need) and the performance of the available systems and applications which may not always match exactly. Therefore any successful information management strategy requires:

- a strategic vision that covers the needs for current, future and legacy information
- time and resources to support:
    - raining and implementation
    - technology, process and business analysis
    - ongoing management activity

1. User focus

Policies, processes and supporting technology must be user focused to eliminate barriers to use.

- Adopting any application or development of an information management policy or process that presents barriers between users and the way they need to access information creates a risk that alternative ways of working will be sought. This can lead to:
    - wasted costs of procurement and implementation
    - individual information repositories outside of a central corporate control or governance
    - information not being properly understood because it cannot be related to information within separate repositories
    - an inability to comply with information legislation and / or unable to meet official scrutiny
    - short term ‘quick-fixes’ being implemented that don’t resolve long term issues
    - an inability to deliver services or reduction in the quality of services delivered
    - information being used or released that is misleading or incorrect leading to further misinformation, financial or reputational damage
    - users’ time and resources wasted with potential cost implications

Conflicting requirements may exist between different user groups:

- internal (staff needs)
- internal (business needs)
- external organisations and their staff (other departments and government officials, wider public sector organisations and private sector organisations)
- citizens (through services, transparency requests or citizen participation)
- there are also current and future needs across all user groups

2. Governance, ownership and accountability

Information assets, the technology that supports them, and the business requirements, policies, and processes that govern them, must have defined and accountable owners.

- If information assets are not owned and understood their value cannot be effectively released. Ownership of information should include:
    - defined ownership with appropriate oversight and accountability for the information assets' management
    - an accessible governance framework for asset owners that defines the relevant legislation, policy, standards and good practice to ensure effective management of the asset
    - the collaboration and co-ordination of a multi-disciplinary team to oversee the ownership of information assets that includes:
        - information managers
        - ICT managers
        - information assurance and security
        - business change teams
        - business owners, and potentially legal, audit and communications teams in delivering each requirement
- Equally all users need to understand they are accountable for their own actions. They should be aware of the legislative requirements they need to fulfil and their responsibilities in ensuring the business requirements are met.

3. Proportionate use of resources

The time, resource and effort expended on managing information must be proportionate to its value.

- Managing information requires an investment of time, money and people to create appropriate policies and processes and implement suitable systems, security and storage. Information value will differ between users and the business. To avoid disproportionate management of ephemeral information identify the value of information assets and record it in an information asset register

- The value of an information asset can be said to equate to:

    - the content of the asset, especially if sensitive in any way

    - the effort required to keep the asset available, complete and usable

    - the length of time, including any legal requirement, an asset needs to be held by the business

    - the consequences of the asset not being available or being accessed inappropriately

- Where actions and activities are not commensurate with the value of information, the organisation can be exposed to unnecessary cost and create additional burdens on users and the IT infrastructure

- The value of information may change over time, especially aspects of sensitivity. To avoid on-going over-management, periodically review and re-value assessts accordingly

- Placing information value at the heart of the decision making process establishes a framework for good governance, risk management and efficient decision making led by business need

- Making value-led decisions enables pragmatic approaches to information security and appropriate use of applications and storage for information assets. It also supports cost savings by identifying information assets and technology no longer required

- The business value of information may not be commensurate with the cost of maintaining it

4. Applications perform consistently

Applications used to store and manage information assets should operate in a predictable and consistent way.

- Information management applications should operate predictably to ensure users understand how information assets can be accessed, used and managed. Applications should ensure two key attributes are properly maintained
    - the information asset is maintained in a common format that all relevant users can access easily with the available software
    - key information management activities are performed in a reliable and predictable way
- The application should perform these tasks consistently to support:
    - increased efficiencies across an organisation through a common understanding of the outputs of each system or application (for example all disposal criteria across each system and application use the same metadata schema)
    - improved information flows within and outside of the department
    - improved compatibility and interoperability across the IT infrastructure
    - the unified management of different types of asset within across applications
- Consistency is equally supported by the use of:
    - common standards; especially important when these are shared by multiple organisations hoping to share or re-use the asset
    - a common approach to risk mitigation, especially to managing loss of information within the application

5. Digital continuity

The value of information can only be fully realised if each asset has the attributes of availability, completeness and usability (collectively referred to as digital continuity).

- Information is:
    - available when it can be found in a timely manner and opened in a readable form
    - complete when it has context and an assured quality
    - usable when it can be manipulated as required with the user's available technology
- The absence of any one of these three attributes can render the information either effectively lost within the system or not fit for purpose meaning:
    - tasks cannot be carried out and services cannot be delivered
    - information is unavailable for sharing, re-use, publication, transfer or to meet calls for scrutiny
- Understanding the requirements for managing completeness, availability and usability enables a department to:
    - deliver appropriate, cost-effective technology in support of its information assets
    - assess risks to the long term suitability of its technology environment to manage critical information assets
    - make decisions about the release of information for exploitation, re-use or to fulfil obligations for transparency
    - highlight user requirements that the department is not aware of or not planning for and therefore unable to meet
    - understanding and manage technology compatibility issues between the department and external recipients

6. Disposal

Information must be disposed of when no longer required by the business in line with legislative requirements.

- There are legislative requirements for (some) information to be disposed of after a certain length of time (Public Records Act, Data Protection Act)
- Information held for longer than required carries unnecessary risk and cost:
    - excessive costs in terms of software licences, storage, IT support and back-ups
    - excessive storage adding burden to servers, creating inefficiencies
    - increased search times owing to volume of information, potentially causing compliance issues with information legislation
- If information is held and it should have been disposed of to meet legislative requirements, the department may be found to be non-compliant or negligent. In these circumstances the department may face:
    - action from a regulatory body (for example, the Information Commissioner's Office) or official scrutiny (such as a Parliamentary Accounts Committee)
- Where the department is found to be non-compliant or negligent it can incur further actions or penalties, particularly in relation to loss or misuse of personal data

7. Transfer

Applications used to store and manage information assets must enable the transfer of the content, context, value and ownership must be transferable.

- Applications should support the transfer of information assets between:
    - internal systems - version upgrades or migration to new platforms
    - external organisations -either for collaboration or where ownership of the asset is transferred
    - other organisations or platforms - to facilitate the release or publishing of that information
- This should include transfer of the descriptive, structural and management metadata to provide the context and value of the asset to the receiving organisation. Where this is not transferred:
    - the context of the asset may not be able to be fully understood
    - the asset may be rendered unavailable, incomplete or unusable
    - the recipient cannot ascribe an appropriate value to the asset relative to its own information assets and any others transferred

If holding information on behalf of another organisation for any length of time it is equally important to retain this contextual understanding until it is returned to the original owner.

8. Audit and compliance

Information assets are evidence of a department's actions, decisions and processes and may be subject to requests for access or to official scrutiny.

- Applications used to store and manage information must be able to provide reports on or audit trails of all activity associated with assets stored within or managed by it. This is to support information as being maintained as evidence, without which the integrity of the asset could be called into question

- Where a department does not have visibility of the actions assets have been subject to there are significant risks that:

    - departments cannot track whether information has been released either under a Freedom of Information or Data Protection request or for transparency or reuse

    - departments cannot state categorically whether they hold an information asset, whether it has been disposed of whether it may have been disposed of or transferred to another organisation

    - information assets will be inappropriately accessed, deleted or shared

    - the true value of the information in relation to a user's need to access it cannot be determined

The National Archives

Annex A: Mapping of business requirements to key information legislation compliance requirements

Legislation and related codes of practice	Ref	Requirement	Relevant business requirement	Related Codes of practice
Public Records Act 1958	s3(1)	To make arrangements for the **selection** of those public records which ought to be permanently preserved and for their **safe-keeping**	1, 2, 4, 5, 8	S46 Code of practice Good records management practice recommendations
	s3(4)	Public records selected for permanent preservation under this section shall be **transferred** not later than 20 years after their creation either to The National Archives or to such other place of deposit appointed by the Lord Chancellor under this Act (to be amended to 20 under Constitutional Reform and Governance Act s 45 (1) (a))	5, 7, 4, 8	
	s3(4)	Records may be retained after the said period, if in the opinion of the person who is responsible for them		

	s3(6)	Public records not required for permanent preservation should be **destroyed** (after 20 years)	6, 4, 8	
		Records transferred closed to The National Archives must be done so against an agreed exemption under the Freedom of Information Act 2000	7,8	
Data Protection Act 1998	Schedule 1, Part 1	Personal data shall be **processed fairly** and **lawfully** and, in particular, shall not be processed unless authorised/required by or under any enactment, convention or instrument imposing an international obligation on the United Kingdom	2, 4, 8	S46 Code of practice Good records management practice recommendations
	Schedule 1, Part 1	Personal data shall be obtained only for one or more **specified and lawful purposes**, and shall not be further processed in any manner incompatible with that purpose or those purposes	2, 8	
	Schedule 1, Part 1	Personal data shall be **adequate, relevant and not excessive** in relation to the purpose or purposes for which they are processed	2, 8	

	Schedule 1, Part 1	Personal data shall be **accurate** and, where necessary, **kept up to date**	4, 8	
	Schedule 1, Part 1	Personal data processed for any purpose or purposes **shall not be kept for longer than is necessar**y for that purpose or those purposes	6, 8	
	Schedule 1, Part 1	Personal data shall be **processed in accordance with the rights of data subjects** under this Act	2, 8	
	Schedule 1, Part 1	Appropriate technical and organisational measures shall be taken against **unauthorised or unlawful processing** of personal data and against **accidental loss** or **destruction of**, or **damage to**, personal data	2, 4, 5, 8	
	Schedule 1, Part 1	Personal data **shall not be transferred** to a country or territory **outside the European Economic Area** unless that country or territory ensures an **adequate level of protection** for the rights and freedoms of data subjects in relation to the processing of personal data	2, 8	

Freedom of Information Act 2000	s19	**Publish** certain information proactively	1, 2, 4, 5, 7, 8	S45 Code of practice Recommendations for public authorities about their handling of requests S46 Code of practice Good records management practice recommendations
	s1	**Respond** to requests for information. To know what you hold and to be able to provide access to it	1, 2, 4, 5, 7, 8	
Environmental Information Regulations	Part 2, regulation 4	Make environmental **information available proactively**, using easily accessible electronic means whenever possible	1, 2, 4, 5, 7, 8	Code of practice on the discharge of the obligations of public authorities under EIR Good practice recommendations to follow in meeting obligations under the Regulations
	Part 2, regulation 5	**Respond** to requests for environmental information	1, 2, 4, 5, 7, 8	

European Directive on the Re-use of Public Sector Information 2003 The Re-use of Public Sector Information Regulations 2005 **NOTE** new Directive will come into force at the end of 2014 (see below) European Directive on the Re-use of Public Sector Information 2013		Make accessible public sector information **available for re-use:** • under standard, open licences • at marginal cost price • without discrimination • where possible by electronic means	1, 2, 4, 5, 7, 8	
Legal Deposit Libraries Act 2003	s1	A copy of every **published work to be deposited with the British Library** within one month of publication and to other deposit libraries on request	4,7, 8	

The Legal Deposit Libraries (Non-Print Works) Regulations 2013	Part 3, regulation 15	A **copy of every offline work is required to be delivered** to the British Library within one month of publication and to other deposit libraries on request	4, 7, 8	
	Part 3. Regulation 16	**Web harvesting of online work** by British Library and deposit libraries or by alternative delivery method where agreed	4, 7, 8	