The National Archives

Mapping the Technical Dependencies of Information Assets

This guidance relates to:

Stage 1: Plan for action

Stage 2: Define your digital continuity requirements

Stage 3: Assess and address risks to digital continuity

Stage 4: Maintain digital continuity

This guidance should be read **before** you start to manage digital continuity. The full suite of guidance is available on The National Archives' website.

Contents

1 Introduction

Digital continuity is the ability to use your information in the way you need, for as long as you need.

If you do not actively work to ensure digital continuity, your information can easily become unusable. Digital continuity can be put at risk by changes in your organisation, management processes or technology. You need to manage your information carefully over time and through change to maintain the usability you need.

Managing digital continuity protects the information you need to do business. This enables you to operate accountably, legally, effectively and efficiently. It helps you to protect your reputation, make informed decisions, avoid and reduce costs, and deliver better public services. If you lose information because you haven't managed your digital continuity properly, the consequences can be as serious as those of any other information loss.

1.1 What is the purpose of this guidance?

This guidance forms part of a suite of guidance that The National Archives has delivered as part of a digital continuity service for government, in consultation with central government departments.

This document follows on from the companion guidance *Identifying Information Assets and Understanding Business Requirements* which helped your organisation to identify its information assets and business needs. The guidance you are reading now will enable you to complete the second stage of managing digital continuity: mapping these information assets to their technical dependencies.

Reading this will help you to understand:

- **why** you need to identify and map the relationships between the information assets your business requires and your technical environment
- **how** to understand and document the technical dependencies of information assets
- **who** to work with

1.2 Who is this guidance for?

This is a hands-on guide aimed at the Head of IT or similar role. It will help you understand and document the technical dependencies of the information required by the business. As the Head of Information Technology (IT), you are ultimately responsible for this process but other members of your team, as well as information managers and change managers, are also likely to be involved in carrying it out (see section 4.4 for more on the roles and responsibilities).

2 Why map your technical dependencies?

Digital information is complex. You need to fully understand its associated business needs and how these needs are met. If you do not know how your technology supports your information you are at risk of losing the ability to **find**, **open**, **work with**, **understand** and **trust** your information, which could have considerable impact on your ability to carry out your business.

The usability of digital information depends on the technology that is used to create, manage and provide access to it – and it is sensitive to any changes in that technology. System upgrades, changes in file formats, data migration, the introduction of new software and the disposal of old technology can all affect the ability of the business to use its digital information in the way it requires. If you do not understand the impact of these changes on your ability to use information assets, you risk losing digital continuity.

Mapping the technical dependencies of your information enables you to relate your technical environment and your information assets directly to your business needs. This will help you to understand and manage the risks to the continuity of your digital information, manage the impact of change, protect your information appropriately and exploit it fully.

2.1 What does it involve?

Managing digital continuity starts with understanding the value of information (recognising information as an 'asset') and understanding how it is used to deliver business needs (defining 'usability requirements'). If your information and technology support the way the business needs to use information, you have digital continuity (see Figure 1 below). If they don't, you're at risk of losing digital continuity.

Although your current needs may be met, both your technical environment and your business requirements are subject to change. You can apply an understanding of the technical dependencies of your information assets to manage such change effectively.

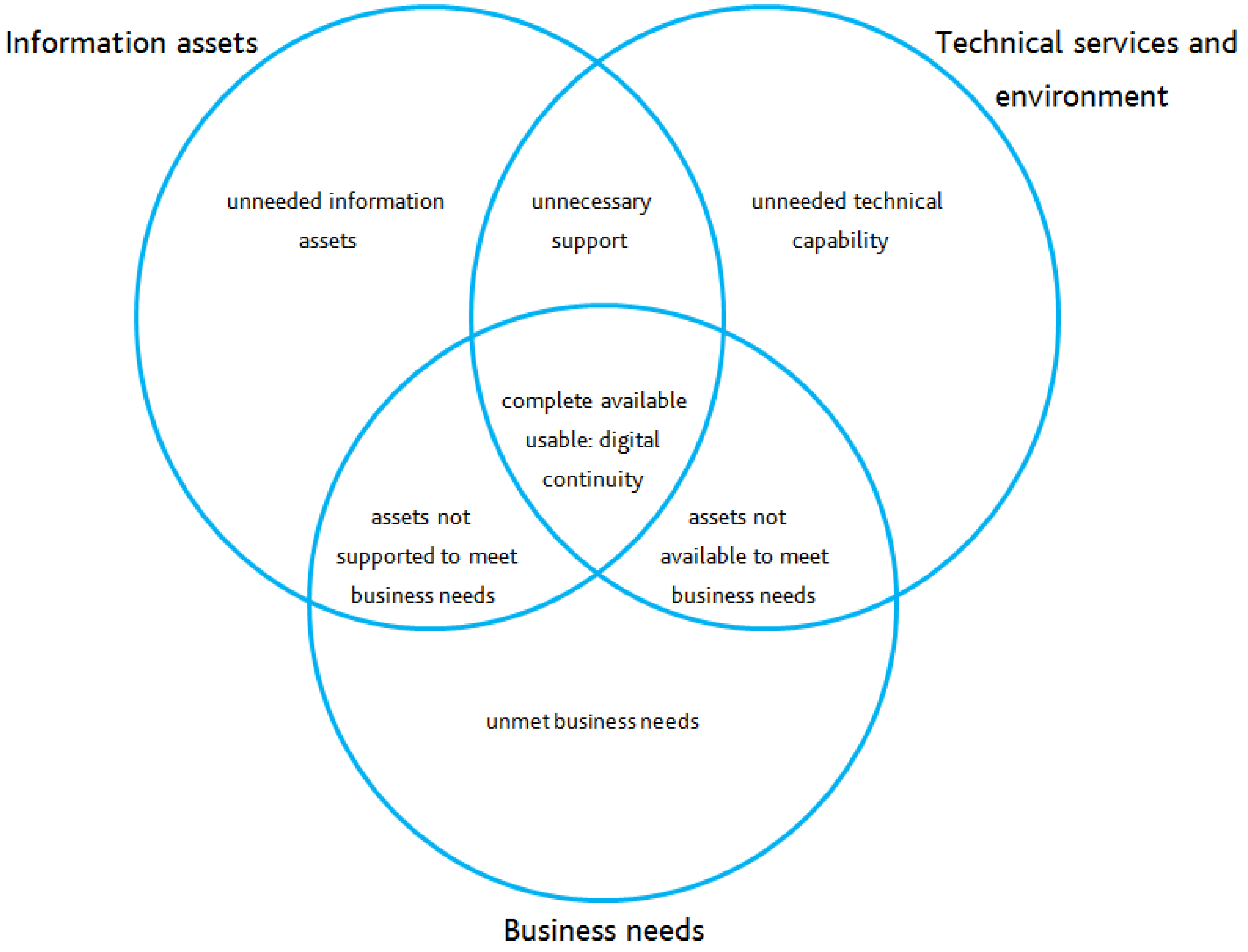
Information assets
Technical services and environment
unneeded information assets
unnecessary support
unneeded technical capability
complete available usable: digital continuity
assets not supported to meet business needs
assets not available to meet business needs
unmet business needs
Business needs

Figure 1: ensuring digital continuity

There are three key steps in understanding and mapping the technical dependencies of information assets:

i. Identify your technical environment
ii. Capture and document technical dependencies
iii. Monitor and review your outputs

Working through these steps in sequence offers the additional benefit of enabling you to build a cycle of continuous improvement.

2.2 What are the benefits?

Understanding which elements of your technical environment support essential information, and which do not, can allow you to streamline your technical environment to remove redundant technology. This can increase IT efficiency and make operational processes more efficient and cost-effective.

It will allow you to:

- make informed decisions about where to prioritise investment to ensure the continued usability of your information
- reveal information or technology you no longer need and highlight where you can make savings by reducing data volumes and streamlining your technologies
- understand whether your technology allows you to use information in the way you need and identify opportunities to improve the service, e.g. where existing technology can improve information management or deliver additional functionality
- identify technical risks relating to managing information assets. The next stage in managing digital continuity is to undertake a full risk and impact assessment to identify specific risks to your digital continuity
- understand the potential impact of change on the continuity of your digital assets

3 Identify the technical environment supporting your information assets

If you have already followed our guidance on *Identifying Information Assets* you will have identified your information assets and your detailed requirements for using them. You may have documented this in the form of an *Information Asset Register* (IAR).

The IAR provides an ideal starting point for mapping the technical dependencies of your information assets. You now need to document how your technology will support the usability requirements which the business has defined for each information asset.

If you do not have a list of assets, or their usability requirements have not been specified, you should now liaise with your information managers and individual Information Asset Owners (IAOs) and encourage them to produce a comprehensive information asset register. Your information managers can use our Information Asset Template as a guide with suggested fields to complete. Your other data repositories may also contain information about your information assets which you can use to create an IAR (see Section 4.1 for more information on how you can use these existing repositories).

3.1 What technical dependencies should you record?

You will need to identify all of the technical systems, platforms and processes which the information requires in order to be fully usable. The easiest way to do this is to start from the list of usability requirements and identify what technical support is needed for each requirement.

In previous guidance on creating an Information Asset Register, we suggested considering usability requirements under five broad categories:

i. How will you find the information?
ii. Who can access the information and how?
iii. What do you need to be able to do with the information?
iv. What do you need to be able to understand about your information?
v. To what extent do you need to trust that your information is what it claims to be?

If your organisation has defined its information requirements in this way, your technology mappings will be similar. Your technical mapping – the information you record, and how you record it – should be tailored to the business needs of your organisation and the processes you use within your department. Below are the five key usability requirements and some suggested questions you should ask when documenting the associated technical dependencies.

Defining usability requirement	Mapping technical dependencies
How do you need to find the information? Consider both granularity and depth of the search required for each type of information asset. Users may need to find the asset itself, files within the asset, or specific pieces of data within the files Consider whether users have different permissions for searching content	What technical tools and services enable users to find the information in the way they need? Include both the technology your users work with directly, and the underlying technology that is used to store, index and retrieve the information. Characteristics of the information assets themselves may also affect find-ability –What is it? Is your data in formats that can be indexed? Is the required descriptive metadata available? –Where is it? Can storage media and storage locations be crawled or indexed by your search technology? Do you require selective indexing? –What applications does the user require to search each information asset? –What indexing services are required? How often are indexes refreshed? –Can the search service manage the required volumes and respond within the required timeframes?
Who needs to access or open the information? How and when do they need to access it? Consider access restrictions and sensitivity. Consider granularity of access controls – do you need to control access to the asset as a whole? To specific files or folders? Or to particular (meta)data elements within the asset? Consider requirements for sharing internally and more widely Consider availability levels and the speed of access required.	What technical tools and services are required to meet access requirements? –How is your technical environment protected from unauthorised access or disclosure? –How are access controls implemented, maintained, reported on? –How are protective markings recorded? How is sensitive or personal data identified and protected? –How are passwords or encryption keys managed? –How is information transferred or shared? –What storage media are used? How quickly can off-line information be retrieved? –What hardware or software allows information to

Consider file formats, encoding or encryption and data structures	be opened or viewed? –Is supporting documentation available? –Can access controls be applied at the required levels? Are they inherited or transferred appropriately when information is created or shared?
How do you need to be able to work with your information? Define the functionality that each group of users requires from your information assets: how they are used and what you need them to do?	What technical tools and services enable users to work with the information? –What file formats or data structures is the information held in? Can these be worked with (viewed, edited, combined, saved)? What interoperability is needed? –What supporting documentation is needed for information held in databases? –Are there specific hardware requirements? e.g. image manipulation may require desktop machines with large amounts of memory –What software is required to use the information in the required ways?
What do you need to understand about the information? You need to understand both the content and context of your information asset. Context may not be recorded as part of the asset itself but is vital to making the asset usable Context is often stored digitally as metadata, but it may also be in linked information, captured within filing structures, or in specific knowledge held by individuals	What technical tools and services maintain the 'context' required to understand the information? –How is metadata associated with the content? –How is context captured within filing structures? –How are links and relationships managed? –Can contextual information be moved or transferred with the content?
To what extent do you need to trust your information? The level of trust required of an information asset varies. Most do not require additional validation –	What technical tools and services support you in protecting your information adequately and deliver the required level of trust? –How do you maintain audit trails which record

they speak for themselves. However, for some uses, you may need to demonstrate the confidentiality or integrity of information assets, or to certify their history and provenance Note: You also only need to map information that provides your defined level of usability – you will not have to do this if you have very low level 'trust' requirements	when information was accessed or changed and by whom? –How do you assure that your security measures are adequate? How do you report on access rights? –How do you capture who created the information and when? How are versions controlled? –How do you manage data quality, accuracy and frequency of updates?

This initial stage of technical mapping involves recording the technologies that directly contribute to the delivery of each usability requirement.

When defining requirements, you should also consider:

- how information moves around your organisation
- how work flows within your organisation

Note: each piece of technology will in turn have its own support requirements and technical dependencies and may also rely on particular documentation, business processes or skills and expertise. It is vital to manage change across the full range of dependencies. Many of these will be captured in separate documentation maintained by your IT department or service provider as part of their configuration management activities. Once you have all these documents in place you will have a full map of your information and the technology it depends upon.

3.2 Where should you record this information?

If your organisation has an existing IAR (or similar spreadsheet or database) we recommend that you record your technical dependencies within this.

Alternatively, you could incorporate this information into an existing Configuration Management Database (CMDB), if your technology organisation has one. With this approach, you should treat each information asset as a Configuration Item (CI), then add attributes to each information CI detailing the technical dependencies.

The principle is to be flexible and practical. The choice of whether to use a CMDB, the IAR or another existing database or spreadsheet will depend on the complexity of your requirements and on the systems that are available to you. The important thing is to make it fit for purpose, and make it work for you. See Section 4.1 for more on how to use existing data repositories to support this work.

4 Capture and document your technical dependencies

In documenting the technical environment which supports your information assets, you should first examine existing sources of data as these can provide you with valuable information. As discussed above, they may also provide a logical place to record dependencies (for instance, in an IAR or CMDB).

To understand the technical dependencies of your information, you will also need to know how this relates to the flow of information around the organisation and the related work processes.

You should also consider:

- the range of tools that can help you understand your technical environment
- who can help you find information and what their responsibilities are

4.1 Key data repositories

The table below lists key repositories which may contain some of the information you require.

Repository	May provide information about
Information Asset Register (IAR)	If you have an IAR it will provide valuable information about information assets and the technology that supports them. Check with your IT support and IAOs that this information is comprehensive and up to date –A description of the information asset –The Information Asset Owner –Technical or systems owners –The date the asset was created or updated –The business value of the information asset –The protective marking attached to the information asset – Retention schedule and disposal schedules – Risks –Locations and systems: storage, hardware, software applications, vendor and platform
Configuration Management Database (CMDB)	A CMDB can be invaluable for discovering the full support system required by an asset and mapping

	how changes to any component may impact upon the information asset –Components of the IT Infrastructure –The IT services supported by that infrastructure –Information about entire services or systems; hardware; software; supporting staff –Documentation
Software registers	–Supported software, versions, product roadmaps, migration schedules –Warranties, support contracts, business ownership, licensing and renewal dates (where appropriate) –Unit cost For example, this information can be found within the Microsoft Enterprise Agreement and the Select Agreement
Hardware registers	This can help you decide the importance of hardware or software to the business, enabling you to manage disposal more effectively. It can also help identify technology approaching end-of-life, or obsolescence –Age –Warranties –Capacity –Spare or replacement stock –Spare or replacement parts –Other dependencies (e.g. disks, power supply)
IT helpdesk data	Primarily for incident management, but can cover problem management, release management and service management – which may relate to information assets (e.g. risks, business impact, locations, dependencies, stakeholders)
Facilities and estates management database	The wider technical and physical infrastructure supporting and securing information assets.

4.2 Key information flows and work flows

Information assets do not remain static, they continuously move around both within organisations and between different ones, so it is important you understand the flow of information and related work processes. This will help you to understand your technical dependencies, as well as informing the development of your organisation's information strategy.

4.2.1 Data flow

As with any other form of inventory, new information is added, moves in and out of central data warehouses, and is eventually decommissioned. Mapping the migration and flow of information around an organisation enables you to identify the network environment and all hardware and software storing or accessing the information, including staging areas where information can be intercepted or restored.

IT management professionals (e.g. network managers, systems managers and database administrators) and IT change managers can track the flow of information assets and identify technical staging areas. Your technical mapping exercise should identify access rights, the location of information assets and catalogue the network environment supporting the information asset.

4.2.2 Work flow

A work flow is a virtual representation of the work an individual or organisational unit actually carries out. It differs from the data flow in that it is designed to identify roles, responsibilities, functions, teams, projects and organisational structures.

Examining work flow can provide you with the opportunity to measure, analyse, identify, standardise, correct, enhance, match and consolidate information assets. It will also enable you to identify weaknesses such as organisational silos and single points of failure.

4.3 Software tools

You will almost certainly have software tools that can help you, even if you don't realise it. Software discovery tools are quite common within organisations and can help locate the software that supports information assets and identify dependencies. This usually falls within the remit of system administrators or system integrators. You should talk to whoever implements your software patching and updates.

Another tool which can help you is DROID, a free file characterisation tool which The National Archives has developed. Through identifying file formats and versions, DROID can help you establish the software dependencies of your information.

A range of related services and solutions are available for procurement via the Digital Continuity Framework.

4.4 Roles and responsibilities

You now need to identify and talk to the right people within your organisation – this will include representatives of information management, IT as well as any external providers or contractors. These individuals will be able to clarify key information and work processes, important management activities and core components of the technical infrastructure, including data repositories. See the Appendix for a full list of roles and responsibilities.

What do you need to do?

As Head of IT, it is your responsibility to maintain an understanding of the way your organisation needs to use its information assets, so that you can ensure that you deliver an adequate level of technical support. You will need to work closely with your information management team to achieve this.

Your understanding of the technical dependencies of information assets will be vital in ensuring that the impact of technical change is understood and managed. It will also enable you to reduce unnecessary support and excess capacity – supporting you in delivering a cost-efficient service.

Communication is vital between everyone involved in looking after information assets and their technical environments. Sharing your findings with other teams will prevent multiple people undertaking the same investigations and improve understanding of how everything fits together.

If your IT service is delivered by external providers, you will still need to ensure that dependencies are captured, documented, reviewed, managed and reported. It is vital to develop good working relationships, establish communication and build a shared understanding of objectives.

5 Monitor and review your outputs

5.1 Understanding how the mapping helps deliver your usability requirements

The real value of the technical mapping is that it allows you to understand how your technical environment supports your key business information. In addition, it provides a number of important management controls over your environment:

Mapping provides:	How it helps deliver your requirements:
Risk controls	Enables you to identify risks to the technology supporting your information asset and prepares you to take mitigating action that is proportionate to the business value of that information For example, gaps such as: absence of software maintenance arrangements, lack of off-site backups, undefined technical ownership, single points of failure will all become apparent as a result of this work. The risks can then be assessed, prioritised and managed
Change controls	Enables you to identify the processes, documentation, people, related (meta)data, software and hardware that impact upon the information asset. This understanding enables effective impact assessment and contingency planning as part of your change process. It enables you to schedule changes and plan upgrades in line with business priorities
Security controls	Enables you to clearly identify security measures in place and to ensure you have a layered solution in keeping with current legislation or international standards
Usability controls	Allows you to understand how your technical environment provides the usability you need (see Section 3.1 above). Allows you to identify excess capacity, unnecessary support, or duplication of functionality

5.2 Measuring against business objectives

Developing an understanding of your information assets and their technical dependencies will enable you to effectively support your information assets over time and through change to maintain their usability – therefore helping you to meet your business objectives.

You should consider how to measure your success in supporting business objectives and set processes in place for reviewing this.

Measurements such as Key Performance Indicators (KPIs) tie in business need with operational change. You can measure the success of your new understanding and against digital continuity-focussed business objectives, such as KPIs based on the availability of information. For instance, this could be the percentage of successful downloads of an information asset within an agreed time frame, or the percentage of relevant search results found by users when looking for specific information.

Be clear about your targets and make sure they are achievable. You will need to work with your information assurance and business managers in order to agree meaningful targets.

5.3 Reviewing and auditing processes

It is important that you continually review your technical environment and information assets, tracking changes that may have wide-reaching impacts. A defined change process should be followed for every change, with impact assessments performed against the IAR. It is also vital to carry out regular audits and compliance checks to ensure that policies and contractual agreements are being followed efficiently and effectively.

You should track your KPI targets to make sure that technical components support the assets appropriately, and take action to improve service levels at all opportunities.

5.4 Reviewing documentation and processes

Related documentation will need to be reviewed on an ongoing basis. This includes:

- Change control documentation – to check that information assets are included in all risk and impact assessments conducted as part of your change management process
- Management documentation, e.g. service level agreements, business plans
- Server documentation and configuration documentation
- Contracts and service levels with external service providers

6 Next steps

Mapping your information assets and their business requirements to your technical environment will help you to manage digital continuity effectively. The next steps are to embed your understanding in operational management, and also to use this mapping to identify risks, exploit opportunities and manage change.

Undertake a risk assessment

With an understanding of your information assets, their business requirements and technical dependencies and how these three elements are aligned, you will be able to identify gaps in the alignment and assess risk to digital continuity. The recommended next stage in the process of managing digital continuity is to conduct a risk assessment, as outlined in our guidance Stage 3: Assess and manage risks to digital continuity.

Read our *Risk Assessment Handbook* for practical information and support to help you assess and manage risks to digital continuity.

Exploit opportunities

Knowing how your current technology supports the information your business values (and needs to support in the future), can enable you to identify redundant or out-of-date technology/technology assets and identify savings and efficiencies for your organisation.

Assess the impact of change

Now that you have a comprehensive understanding of your current information assets, their requirements and technical dependencies, you are well-positioned to assess how change can affect the continuity of your digital information.

You will be able to identify the impact of technology change on the usability of your information assets – ensuring that you manage these changes effectively and reducing the risk of losing access to business critical information. You should improve your change management processes, embedding management of digital continuity into operational practice. See our Machinery of Government (MoG) change guidance suite for more information on how to achieve this.

Appendix

Role	Responsibility
Head of IT	The Head of IT is ultimately responsible for the implementation of technical dependencies to manage the information required by the business. However, other members of your team, as well as information managers and change managers, are also likely to be involved in carrying it out
Head of Knowledge and Information Management (KIM)	The Head of KIM will be able to provide you with information about the organisation's information assets and their business value. The head of KIM will detail all management documents and roles associated with information assets, especially those of the information assurance managers and IAOs
Information Asset Owners (IAOs)	IAOs are responsible for information assets identified in the IAR. Information management representatives such as IAOs should be included in relevant technology meetings, including on change advisory boards
IT Change Manager	Change managers link the work of the IA managers and IAOs with changes to the IT infrastructure –Manage risk and safeguard availability –May own configuration management processes and the CMDB if they exist –Work as information asset champions with ICT and can track and manage all technical risks and impacts upon the IAR –Will work with external service delivery partners to ensure all changes follow an agreed process in order to meet agreed availability and KPI targets
Configuration Manager	Manages the Configuration Management System (CMS) and the Configuration Management process. Many government departments do not have a CMS, or they might not realise it, as the CMS could be part of an outsourced service delivery. If there is a

	Configuration Manager this person will be working closely with the Change Manager
Service Level Managers	Work alongside Heads of KIM to attach an appropriate service level to information assets and continuously monitor and report to maintain availability and security targets. This is best achieved by establishing a service level for the IAR. Service Level Managers will manage external service delivery partners along with the Change Manager, and ensure all relevant availability and KPI targets are being met
Operational IT professionals	Regardless of whether an organisation has contracted out its IT services there will be technical support roles managing key technical components. These include: –System managers –Database and application managers –Database administrators –Network managers –Network administrators
External providers/contractors	Maintaining and managing the IAR should be included in the procurement requirements for external providers and included in any subsequent contracts. Changes impacting upon the IAR should follow defined operational change management procedures. Technical points of contact are should be identified in all contracts