Best Management Practice
For Portfolio, Programme, Project, Value, Risk and Service Management

OGC

ITIL® Managing Digital Information Assets

Shirley Lacy, ConnectSphere

Frieda Midgley, Digital Continuity Project

Judith Riley, Digital Continuity Project

Nigel Williamson, Digital Continuity Project

The National Archives

ConnectSphere
Deliver Success

White Paper
January 2011

Contents

Synopsis

Information is a valuable asset and needs to be managed as carefully as any other tangible asset, such as money or equipment. In particular, you need to ensure that digital information assets can be used as needed, for as long as needed, to support business requirements. This is called managing digital continuity.

This White Paper uses ITIL service management best practices to explain the principles of providing services to business customers that are fit for purpose, stable and reliable. It is complementary guidance to ITIL on digital continuity.

This paper explains what IT service providers, and key points of contact with external IT suppliers, need to do to manage digital continuity in relation to their business activities.

In brief, you need to take action to make sure that your technical environment adequately supports the digital information your organization relies on. That means making sure it supports the way your organization needs to use its information, and provides sufficient functionality now and in the future.

Key recommendations are as follows:

- Understand what information the business needs and how that information is used in a business context.
- Define information assets by content and business use rather than by what system holds the information.
- Define the scope of your information asset register (IAR). Design it, then use it to improve the way you manage your digital information.
- Use your IAR to help you to understand and record the relationships and dependencies between your information assets, business requirements and technical environment.
- Use your IAR when contracting with new IT service providers, to ensure good information asset management. Through the active management of the IAR in the IT services contract, information assets become true configuration items. This will help you to effectively manage and maintain digital continuity, reducing risks as the technology and the organization itself change.

As part of good information asset management we also recommend that you assess the impact of asset, business or IT change on digital continuity. Good change management is essential if you are to ensure your information assets continue to support your business requirements.

For more information visit **www.nationalarchives.gov.uk/digitalcontinuity.**

This White Paper provides complementary guidance to ITIL. For more information visit **www.itil-officialsite.com.**

Introduction

> *'Information is a valuable asset that must be safeguarded. In the case of information held by public authorities and businesses … people want to be certain that it is held securely, maintained accurately, available when necessary and used appropriately'*
> Sir Richard Mottram, Foreword, National Information Assurance Strategy

Organizations depend on digital information to manage and operate their business. This makes information an asset that needs managing and protecting as carefully as more tangible assets such as money or equipment. If you manage your information assets well, you can operate legally and accountably, improve customer and public services, and save or avoid costs. Information asset management can deliver IT efficiencies. It helps you to identify where you are providing unnecessary support or where you have under-utilized capability.

If you do not manage your information assets well, you could lose business-critical digital information. You could also lose the ability to use digital information as you need to, with all the associated financial and reputational costs. You could be storing information that has no business value – and although technology allows us to store more and more information cost-effectively, this has knock-on costs which continue to grow. These include the increased costs of maintaining and backing up the data, and the need for more expensive technologies to find and retrieve the right information in a timely fashion.

This White Paper provides introductory guidance for IT providers, complementing ITIL guidance[1]. It explains how IT can support the management of digital continuity; that is, the ability to use digital information as needed, over time and following change.

It provides guidance on how to manage digital information assets across an IT service supply chain. This includes what you can do to identify opportunities and manage risk.

It explains what we mean by information assets, and introduces the basic concepts and principles of managing them. It includes advice on why and how to manage digital information assets as a configuration item, linking into the information asset and configuration management responsibilities covered in ITIL.

It outlines the obligations for contractors to maintain an IAR for the duration of their contracts. It also summarizes key recommendations from the UK government's Digital Continuity Project[2].

---

[1] ITIL is a Registered Trade Mark, and a Registered Community Trade Mark of the Office of Government Commerce, and is registered in the US Patent and Trademark Office. ITIL is a collection of best practice guidance on the management of IT services. It is a comprehensive framework from which organizations, and their agents, can adopt and adapt their own practices and procedures.

[2] The Digital Continuity Project is funded by central government and managed by The National Archives. It is developing a service that will help you to ensure digital information is usable over time, and following change. For more information visit www.nationalarchives.gov.uk/digitalcontinuity.

This White Paper will also be of use to anyone interested in managing digital information assets in central government, the wider public sector, and commercial organizations.

ITIL service management best practices referenced in this White Paper

- Managing services through the service lifecycle
- Service portfolio and service catalogue management
- Financial management
- Demand management
- Capacity management
- Service level management
- Information security management
- IT service continuity management
- Availability management
- Service asset and configuration management
- Change management
- Incident management

1 Information asset management

An **information asset** is information held by an organization, categorized from the perspective of its content and business use rather than by the IT system that holds it. An information asset is information that has been grouped in a way that enables you to protect, manage, share and exploit it effectively. An organization will need to decide how to group its information to ensure that the asset is both useful and able to be effectively managed. An information asset can contain structured or unstructured information and may range from a single file to many files.

Information asset management is the effective management, control and protection of information assets within an organization. Asset management is the process responsible for tracking and reporting the value and ownership of assets throughout their lifecycle.

1.1 Why manage information assets?

Information can be a valuable asset, and it needs to be managed as such. In this digital age, managing information assets requires input and support from IT and the people responsible for knowledge and information in the organization.

Good information asset management protects the information your business relies on – and that means you can operate legally and accountably, and take informed decisions. It protects you from risk – the risk that you will lose information, or lose the functionality required to use the information you have to support your business requirements.

Specific IT benefits include:

- Understanding where you are maintaining IT to support information no longer required by the organization. This will enable you to take evidence-based cost-saving decisions; for example, on standardizing applications and software, or reducing the number of licences you pay for
- The potential for reducing storage costs. If you are keeping only the information your business needs, this could lead to reduced back-up costs and time savings, reduced electricity costs and a need for fewer servers
- A clearer understanding of how your technical environment needs to support the business. You will be helping to ensure that business-critical information is usable, i.e. that you are maintaining the required level of functionality
- More effective use of your IAR, with clearer responsibilities for IT service providers, their customers, suppliers and business sponsors.

2 What are the digital challenges?

Understanding the digital challenges for each specific business context helps all the parties to work together and map information assets to business need.

2.1 Adapting to manage the growth in digital content and information

Factors driving the growth of information include the increased computerization of businesses, the improved ease of use, the decreasing cost and increased availability of digital technology, and internet applications for e-commerce and customer support. This growth causes many challenges for IT teams, such as:

- Adopting new technologies and techniques to search, store and secure digital information
- Supplying the right capacity at the right cost as the business information needs and technology change
- Adapting to store and manage digital content and information assets effectively and efficiently
- Meeting the green IT agenda during the rapid growth in digital information

- Developing strategies to manage digital information effectively throughout its lifecycle.

2.2 Understanding how digital information supports the business

Users need information to work efficiently to deliver business benefits effectively, and to operate legally, accountably and transparently. One challenge is to know what information is required, when, where, by whom, and how it is used (now and in the future); also, how the underlying IT services and infrastructure support the delivery of information to users over time and through change.

2.3 Identifying digital information assets and their relationships

Information is used in many ways and in many formats, through different channels and interfaces. The challenge is to identify information assets, their relationships and dependencies. Without this understanding, it is difficult to manage the costs and other impacts of change on information assets.

2.4 Ensuring digital continuity through business and technology change

Digital information is particularly vulnerable to change. It is reliant on complex systems, formats and media to support it, and the expertise and understanding of the people who manage it. Although organizations have procedures to protect and back up digital data, these will not necessarily ensure the continuing completeness, availability and usability of digital information. They cannot protect against changes in the business and technical environments. The challenge is to ensure that you can use digital information in the way that you need to as the underlying IT changes, digital information ages, and organizational structures and business needs change.

2.5 Managing the liabilities and risks associated with information assets

Information that is not usable or disposed of at the appropriate time can become a financial, reputational and legal liability; for example, where there are concerns about privacy, security, and intellectual property protection associated with digital information assets.

2.6 Managing information across the supply chain

Delivering services in today's world often involves activities that are carried out by multiple suppliers. This adds to the complexity of the responsibilities and processes involved in managing data and information across a supply chain.

2.7 Reducing redundancy and duplication, and disposing of information

With the complexity of systems and IT services it is often difficult to know what information to keep. Organizations often either lack the confidence to make decisions and take action on what to dispose of or archive, or they do not yet have in place the systems and procedures to enable them to do this.

3 Where digital continuity fits in

Complete This means that everything you need to use and understand the information is there, including the content and context, such as metadata – so, for example, you still have links to external files or you have maintained important connections between files and metadata.

Available This means you can find what you need and that it can be opened with available technology – so, for example, you have the metadata you need, or you have information in versions that can be processed using available IT applications.

Usable This means that it is fit for purpose and can be used in a way that meets the business needs of the organization – so, for example, information is not locked into formats or systems that restrict your ability to use or reuse it, or that restrict the tools you can use to process it.

Digital continuity is the ability to use digital information for as long as needed, to meet business requirements. Managing digital continuity means making sure that anyone who needs information can identify it, retrieve a copy, read, or otherwise use the content as required. They will also be confident that the information is complete, available and usable. To achieve this you will need to make sure that your business needs, your information assets and your technical services are aligned (see Figure 1).

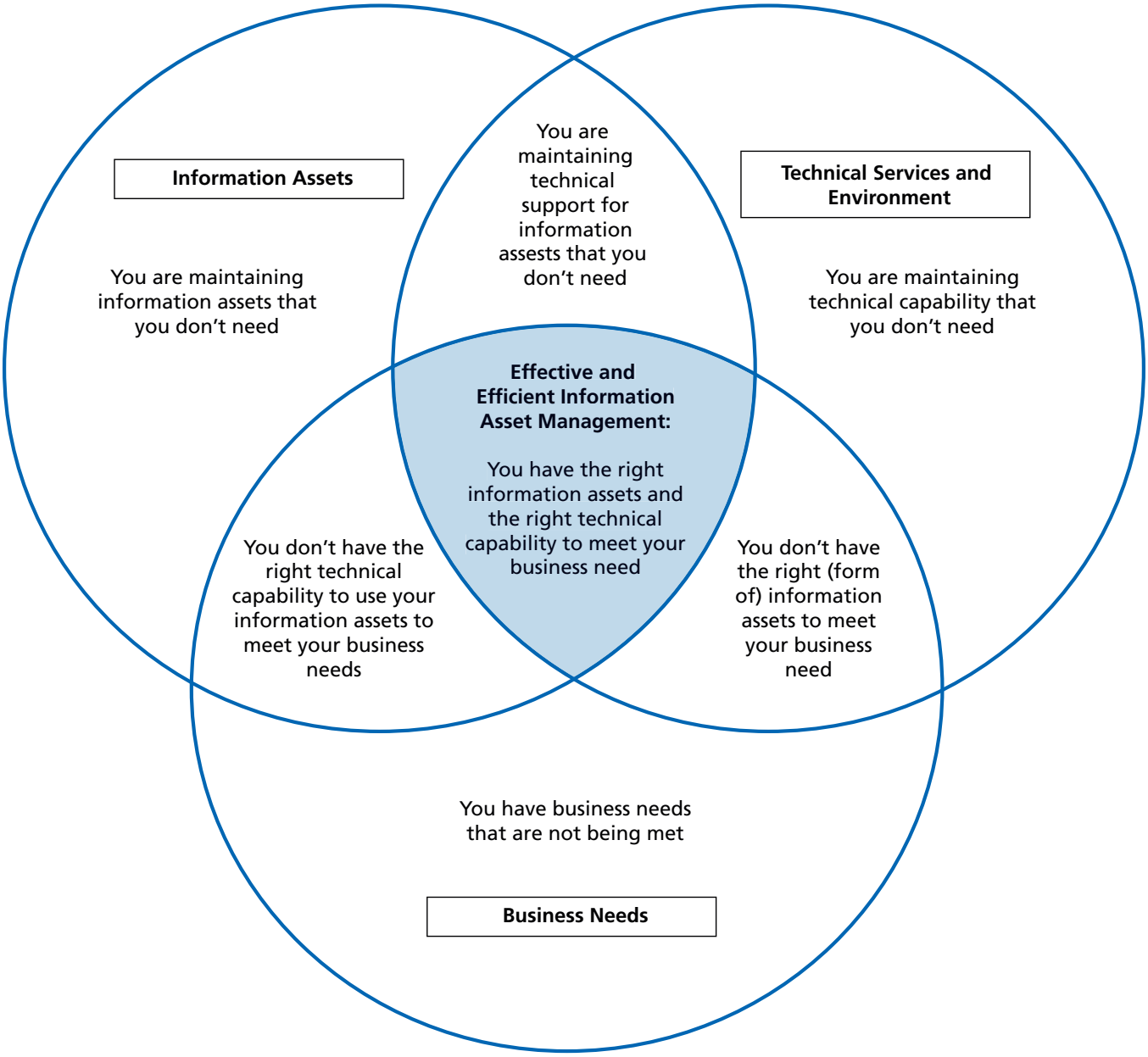

Figure 1 Effective and efficient information asset management

Digital continuity is about managing digital information through change. Change of any kind puts digital information at risk, because it alters the alignment between your business requirements, your information and your technical environment. When these things move out of alignment, you might lose digital information, or the ability to use it as you need to.

3.1 Business or organizational change

If your organization is given new responsibilities, for example, you might be required to do new things with your information. If your IT or information management do not allow that to happen, then you are at risk of losing digital continuity. That could be for a variety of reasons. Perhaps your IT service contract is not flexible enough, so making changes to meet your new needs is too expensive. Or perhaps your metadata policy is now inadequate, because it does not provide the rigorous audit trail you now require.

3.2 Technical change

Changes to your IT environment can also impact on digital continuity. You can lose essential bits of your information, such as metadata, during transfer to a new IT system. Or you could lose functionality if formats or applications are no longer supported or are upgraded.

Technologies can also become obsolete. If you do not have a plan in place to migrate at-risk information to new formats or systems that provide the functionality you need, you could easily lose digital continuity.

Managing digital continuity means defining and managing information from a content perspective and a technology perspective.

3.3 Identifying business needs and technical dependencies

Effective management of digital information assets means that you have the right capabilities and resources to meet your ongoing business needs, as shown in Figure 1.

This requires that:

- You understand how your organization needs to use its information to support its business requirements (i.e. what information you need, for how long, who needs to use it and in what way)
- You then make sure that your technical environment and the way you manage your information assets support the identified business requirements.

Your IT should provide support for your information assets in the way you need to use them – not just today, but as business needs and technology change, and digital information ages.

The National Archives' Digital Continuity project is developing a service for the public sector that will support digital continuity management. You can find guidance at **www.nationalarchives.gov.uk/recordsmanagement/dc-guidance.htm**

3.4 ITIL principles that support digital continuity management

ITIL defines a 'service' as a means of delivering value to customers by facilitating the outcomes that customers want to achieve without the ownership of specific costs and risks.

If we consider a business service such as 'payments', the business outcomes are making the right payments on time, with the expected resources, and without any unexpected costs or risk. The 'payments' business services are supported by a number of technology services such as 'information access administration', 'database service' and 'storage administration'. Managing the entire business service along with its underlying components ensures that we are delivering the required functionality (or utility – i.e. accurate payments) and service levels (or warranty) to the business customer.

Managing digital continuity is about making sure that your technical environment supports your organization to use its digital information assets as it needs to, now and in the future. This fits with the ITIL principles of delivering service utility and warranty:

- **Utility** Delivering a service that has a positive effect on the performance of tasks associated with desired business outcomes. This is **fitness for purpose.**
- **Warranty** The positive effect is available when needed, in sufficient capacity or magnitude, and dependable in terms of continuity and security. This is **fitness for use.**

The following examples illustrate how ITIL is used by many IT service providers to ensure that the warranty is delivered:

- **Demand management** and **capacity management** to ensure that sufficient capacity is provided to deliver the current and future demand for services; for example, payment workload and digital storage needs
- **Service level management** to ensure that agreed service level targets can be met; for example, performance levels for a specified workload
- **IT service continuity management** to support business continuity
- **Availability management** to ensure that all IT components are appropriate to deliver the agreed service level targets
- **Information security management** to ensure the confidentiality, integrity and availability of an organization's assets, information, data and IT services
- **Incident management** to restore service as quickly as possible to users.

Managing digital continuity will help you to ensure that the utility and warranty you are providing support the ongoing use of digital information to fulfil business requirements, at the right cost.

3.5 Organizing for digital continuity

Digital continuity should fit within a wider spectrum of activity within your organization, including the appointment of a senior sponsor for digital continuity who champions governance. The senior sponsor may delegate responsibility for this to someone like a chief information officer, head of knowledge and information management or chief technology officer – that is, someone who has the authority to escalate issues to board level if required. Your organization may also have information asset owners – senior individuals who have been given additional responsibility for managing information risk. Every organization is different, and job titles may vary.

We recommend that you work closely with other disciplines to manage digital continuity effectively. Find out who is responsible for knowledge and information in your organization – they should understand their information assets and map them against business requirements. You could also talk to your enterprise architects or strategists, your information assurance specialists, the people responsible for change management, and procurement or contract managers.

Annex C provides more detail on these roles and their responsibilities, and how what they do can support you.

3.6 Financial management and service portfolio management

Financial management provides the business and IT with the quantification, in financial terms, of the value of IT services, the value of the assets used to provide those services, and operational forecasts.

In ITIL, service portfolio management helps organizations to consider all the relevant factors when deciding which IT services to offer to which customers and which to withdraw from their service portfolio. Robust service portfolio management must factor in digital continuity. The process of managing digital continuity will enable you to understand where your technology is supporting unneeded information, where essential information assets are not adequately supported by technology (or are likely to become unsupported; for example, as a result of technological obsolescence or changes to systems and contracts), and where technology could improve information asset usability.

The service portfolio can be a valuable tool in decision making, supporting you to manage changes to information assets, model the resource requirements required to manage information assets and deliver digital continuity. Within the service portfolio, the view of the operational services is the service catalogue.

The service catalogue management process ensures that information in the catalogue is accurate and reflects the current details, status, interfaces and dependencies of all services that are being run or being prepared to run in the live environment. It helps to set the customers' expectations of the value and potential of their IT service providers.

4 Using your IAR to understand the relationships between your information assets, business requirements, and technical environment

The five stages shown in Figure 2 provide a framework of the actions your organization can take to help you assess and improve the management of your digital information assets (for more detail see Annex C). One of the principal ways you can manage your digital information assets is by adapting your IAR.

The IAR is a conceptual rather than a physical entity. In practice, your IAR is likely to consist of a number of separate registers, documenting particular aspects of your digital information and its environments. It might build on existing lists of information assets or use the ITIL service asset and configuration management process to link the various elements. This does not matter, as long as you can understand what information assets you have, how the business needs to use them, the technical dependencies between them, and you can identify the information assets dependent on each component of your technical environment. Whatever way you develop your IAR, you need to be able to use it to assess and manage the impact of change.

Within an IT services environment, the IAR identifies the information assets as distinct configuration items which relate to the technology that enables them and the business outcomes that they are required to support. Once the IT services IAR is under active management (including with outsourced IT suppliers), any impacts on the information assets can be

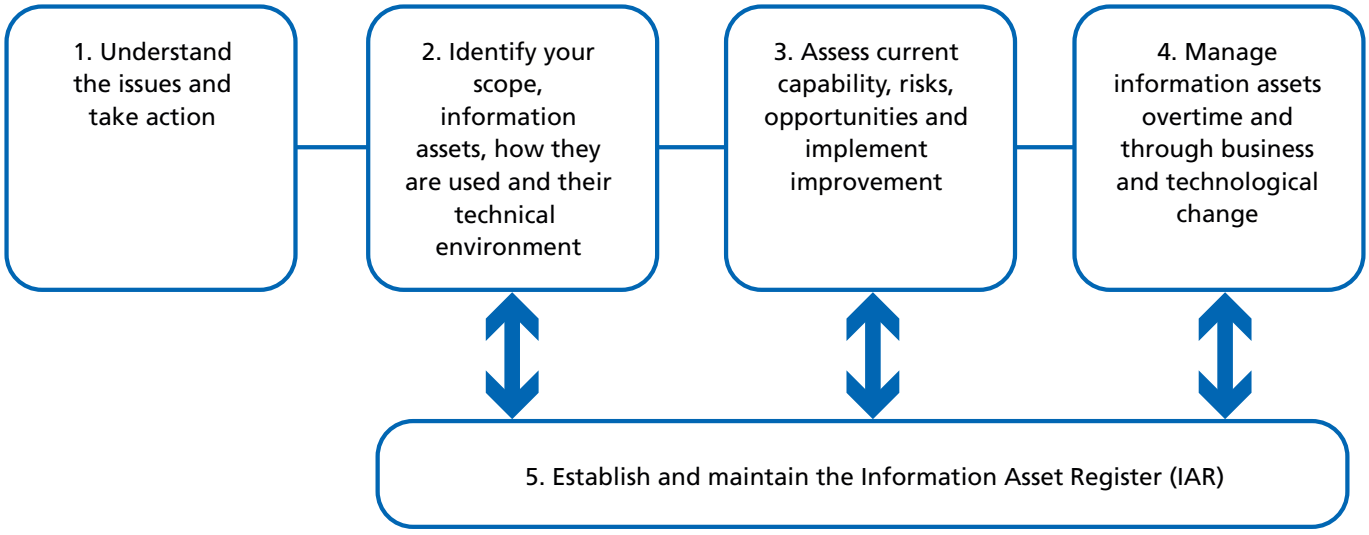

Figure 2 Key steps to improve the management of your information assets

more easily assessed at times of change. This ensures that the business outcomes continue to be delivered, both at the time of the change and for the duration of the IT services contract.

4.1 Defining the scope of your IAR and identifying starting points

- Which information assets are you going to focus on initially? Are there priority areas of the business, IT services or key information assets that should be tackled first? For example, new or business-critical services, their applications and information assets and technology platform.
- What level of detail do you require? You may want to start with a high-level overview, and take a phased approach to developing the underlying detail.
- Are there plans to change or implement information systems that would provide opportunities for developing sections of your IAR?
- Are you due to renew or replace your service contract?
- Do you already have components of the IAR in place that could be built upon?

4.2 Designing your IAR

- Decide how you will identify your information assets. How will you define and classify them? How will you ensure that each one you identify is unique? Who is the business owner of each one? How will you quantify the value they provide to the business? What do they cost to create and maintain? Work with your knowledge and information management team to understand what is currently being done and whether it meets business needs. Roles are defined in Annex B. If you do not have these specific roles in your organization, find someone who has similar responsibilities or skills.
- Document the information asset content and context, where the information is located, its current format and structure, and relate this to the technical environment that supports it.
- Ensure that your IAR allows you to link what you know about the business value and utility requirements of your information asset with what you know about its technical characteristics. This will inform decisions about how to manage the continuity of your digital information assets through change.
- Ensure that you can also understand what information assets are dependent on each component of your technical environment, so that you can see which information assets may be affected by changes to your technology.
- Establish processes for updating this mapping, with regular review periods to audit for completeness and effectiveness.
- Ensure that ownership and responsibility for maintaining the IAR itself is clear. Ownership will probably rest with your senior sponsor. Responsibility for maintenance will probably be shared between the information assurance function and the information asset owners in the business, as appropriate.

Case Study 1

An IT service provider did not understand how digital information flowed through the business and suspected there was a lot of duplication of information within applications. It also wanted to use this knowledge to manage its IT assets more cost-effectively, and to ensure that it was supporting information that had real business value, rather than storing huge volumes of data.

The service provider achieved this by establishing a new configuration management system (CMS). As part of the initial project assessment, data on digital information assets, business services, IT services, applications and the rest of the technical environment was gathered. It found that there were over 200 applications in use, and for one application each division had its own name for the same application. Once the CMS was established it was easier to understand the impact of changing technology on the information assets. So when the time came to upgrade key applications, the need to migrate information contents and keep them usable was flagged and actioned.

The asset and configuration manager used the following ITIL categories to help identify and categorize configuration items (CIs) more effectively:

- Service lifecycle CIs that provide a picture of the service provider's services, how these services will be delivered, what benefits are expected, at what cost, and when they will be realized
- Service CIs such as:
  - Service capability assets: management, organization, processes, knowledge, people
  - Service resource assets: financial capital, systems, applications, information, data, infrastructure and facilities, financial capital, people
  - Service and process models
  - Service package and service design package
  - Release package
  - Service acceptance criteria
- Organization CIs – Some documentation will define the characteristics of a CI, whereas other documentation will be a CI in its own right and will need to be controlled; for example, the organization's business strategy or policies
- Internal CIs comprising those delivered by individual projects
- External CIs such as external services, external customer or third-party requirements and agreements, releases from suppliers or subcontractors
- Interface CIs that are required to deliver the end-to-end service across a service provider interface.

The system was used on an operational basis to manage information assets through technical, organizational and business change.

4.3 Adopting the ITIL asset and configuration management practices with the IAR

Many organizations have implemented the ITIL asset and configuration management process as a way of maintaining information about the configuration items required to deliver an IT service, including their relationships with each other. This configuration information is managed throughout the lifecycle of the configuration item (for example, information asset). Changes to every configuration item are approved through the ITIL change management process. Implementing the change includes updating the relevant configuration records, such as the IAR.

Service providers that manage large and complex IT services and infrastructures use a supporting system known as the configuration management system (CMS). The CMS holds all the information about CIs within the designated scope. For example, a service CI (such as a web service) will include the details such as supplier, cost, purchase date, renewal date for licences and maintenance contracts, and it will be linked to controlled documentation such as agreements and contracts. The CMS maintains the relationships between all service components and records for all related changes. At the data level, the CMS will provide access to data in asset registers, wherever possible, rather than duplicating data.

You need to expand ITIL asset and configuration management approaches to include information assets as configuration items. If you use a CMS make sure you include information assets, such as web content, too.

5 Using the IAR to improve the way you manage digital information

Once you have established an IAR covering some or all of your information assets, you can begin to use it to improve your management of digital information, as follows.

5.1 Planning for effective and efficient information asset management

- Use the mappings of dependencies in your IAR to understand the potential impact of organizational or system change.
- Ensure that your enterprise architecture planning and implementation reflect the business requirements for your information assets and the need to ensure you can still use digital information after technical, organizational, or business change.
- Use your understanding of the impact of change to build a consideration of the long-term use you need from information assets into IT system design and development, to minimize the impact and cost of change.
- Use your understanding of the impact of change to plan the migration of information assets to standardized technology and open standards, wherever possible. This will ensure information assets are future-proofed and less at risk from change.
- Use your understanding of the impact of change to identify where you can standardize the technology, software, environment and formats you use to minimize reliance on bespoke systems, proprietary software or complex formats. This will make your technology environment easier to manage and ensure that changes have minimal impact on digital continuity.

5.2 Identifying risks to digital continuity

- Identify the information assets that you need to use, but are currently insufficiently supported by the right technology and so do not efficiently meet your business requirements – this is an area of risk to your digital continuity.
- Assess the impact of business and technology change on the usability of digital information.
- Identify potential points of failure and vulnerability when designing the availability and continuity for new and changed services.

Case Study 2

A consultant helped a bank, a city council and a rail operator to establish a strategy for digital continuity that would guarantee the availability of key IT services during business and technology change projects. In the first phase, ITIL best practices were used to:

- Establish a service portfolio management process. The process ensured that the investment case for proposed new and changed services covered all the lifecycle costs of the service including: maintenance, up to three platform and format changes during the lifetime of the service, and a budget for disposal of service assets including the information assets.
- Integrate the existing IT change management process with the IAR and the CMS to provide a solid framework for managing changes to all digital information assets.
- Manage all changes to the IAR and their storage locations through the IT change management.
- Establish a process to check the progress of projects against agreed financial targets, risk profile, business utility requirements and the service level targets process as services progressed through service design, service transition and into live operation.
- Improve the supplier management process to ensure that all new and changed contracts with third parties clearly defined the accountability and responsibilities of both parties when managing changes to IT services, the technical environment and updating the information asset register.

5.3 Identifying and planning the realization of savings and efficiencies

- Identify information assets that are no longer required to meet your business needs (or no longer required in their current form), and technology capability and support that are no longer required.
- Dispose of any information assets that you no longer need.
- Dispose of any technology capability that you no longer need.
- Identify opportunities to downgrade the technology you use to access information or migrate information to different formats, so that your technology mirrors your needs, saving money on expensive systems, unnecessary functionality or high availability.
- Move the information assets to cheaper, more efficient and effective storage, de-duplicating assets.

5.4 Contracting with new IT service providers

- Through the active management of the IAR in the IT services contract, the information assets become true configuration items and the organization is able to effectively manage and maintain digital continuity, reducing risks as the technology and the organization itself change.
- The OGC model agreement for IT services now includes reference to an IAR as one of the registers to be maintained as part of the service configuration management. The IAR needs to be created by the contracting authority. It is then maintained by the contractor, who has to assess the impact of any changes on the usability requirements defined for the information assets.
- In the contract service description, the services must be mapped to the information assets that relate to the delivery of that service in order to deliver the utility (i.e. business outcomes) required.
- The IAR should be initially created by the contracting authority prior to procurement, used in the due diligence process and updated or refined during the contract negotiations.
- Once the IT services contract is in place, the IAR is referenced from the contract, and is maintained by the contactor. The model contract contains several clauses which detail rights or responsibilities in relation to the IAR. In summary they are as follows:
  - The contractor is obligated to ensure that the IAR is maintained.
  - Any changes to the IAR should go through the operational change procedure or the contract change procedure.
  - All changes which go through the operational change procedure or the contract change procedure will explicitly address the impact on the IAR.
  - The authority has the right to audit the IAR for completeness and accuracy.

5.5 Obligations on suppliers to use an IAR when contracting for IT services

The OGC model agreement for ICT services includes an obligation for the contractor to maintain an IAR for the duration of the contract. There also needs to be agreement on the approach to:

- Managing changes to the IT services, technology environments and information assets between the contractor and the authority[3]
- Sharing asset and configuration management information where this facilitates more effective change planning and impact assessment of changes.

Benefits of using an IAR when contracting for IT services

The following benefits for both the contractor and the contracting authority can be derived from using the IAR during procurement and management of IT services:

- Clear definition of the information assets that a new contractor will be expected to support in relation to delivering the service, leading to clarity and understanding between both parties on the service provision.
- Appropriate service design that fully meets business requirements for information and that takes into account any legacy technology issues.
- The flexibility required to keep digital information usable is built in to service design, so making change less costly – for example, by moving towards open standards-based design, rather than bespoke systems.
- Early identification of potential digital continuity issues during procurement, leading to agreement on issue resolutions during the solution design phase rather than relying on post-contract change control – this is more economic and carries a lower technical risk.
- Improved ability to make joint decisions about IT changes.
- Greater change success rate; changes can be implemented effectively and efficiently with minimal disruption to the live services.
- Greater ability to identify and eliminate redundant data, leading to cost and process savings.
- Greater ability to identify redundant licensing, leading to cost and process savings.
- Greater ability to identify uneconomic subsystems, leading to cost and process savings by identifying alternative file formats and licensing options.
- Reduced risk of inadvertent digital continuity issues being introduced by change through the life of the agreement.
- Once the IAR exists it can be used in subsequent procurements and due diligence exercises.

[3] By 'authority' and 'contracting authority' we mean the organization contracting the services required.

6 Manage information assets over time, and during periods of change

As part of good information asset management you must assess the impact of asset, business management or IT change on digital continuity and the availability of IT services to ensure your information assets continue to support your business needs and to reduce the likelihood of continuity issues arising. Figure 3 shows how to use the ITIL service lifecycle to achieve this.

6.1 Using the ITIL service lifecycle to manage digital continuity

Many organizations are adopting the ITIL service lifecycle (see Figure 3) to enable them to manage business and technology changes more effectively and efficiently. You can use the ITIL service lifecycle to help you to manage digital information assets through business and technology change.

The service lifecycle contains five elements as shown in Figure 3, each of which rely on service principles, processes, roles and performance measures. Each part of the lifecycle exerts

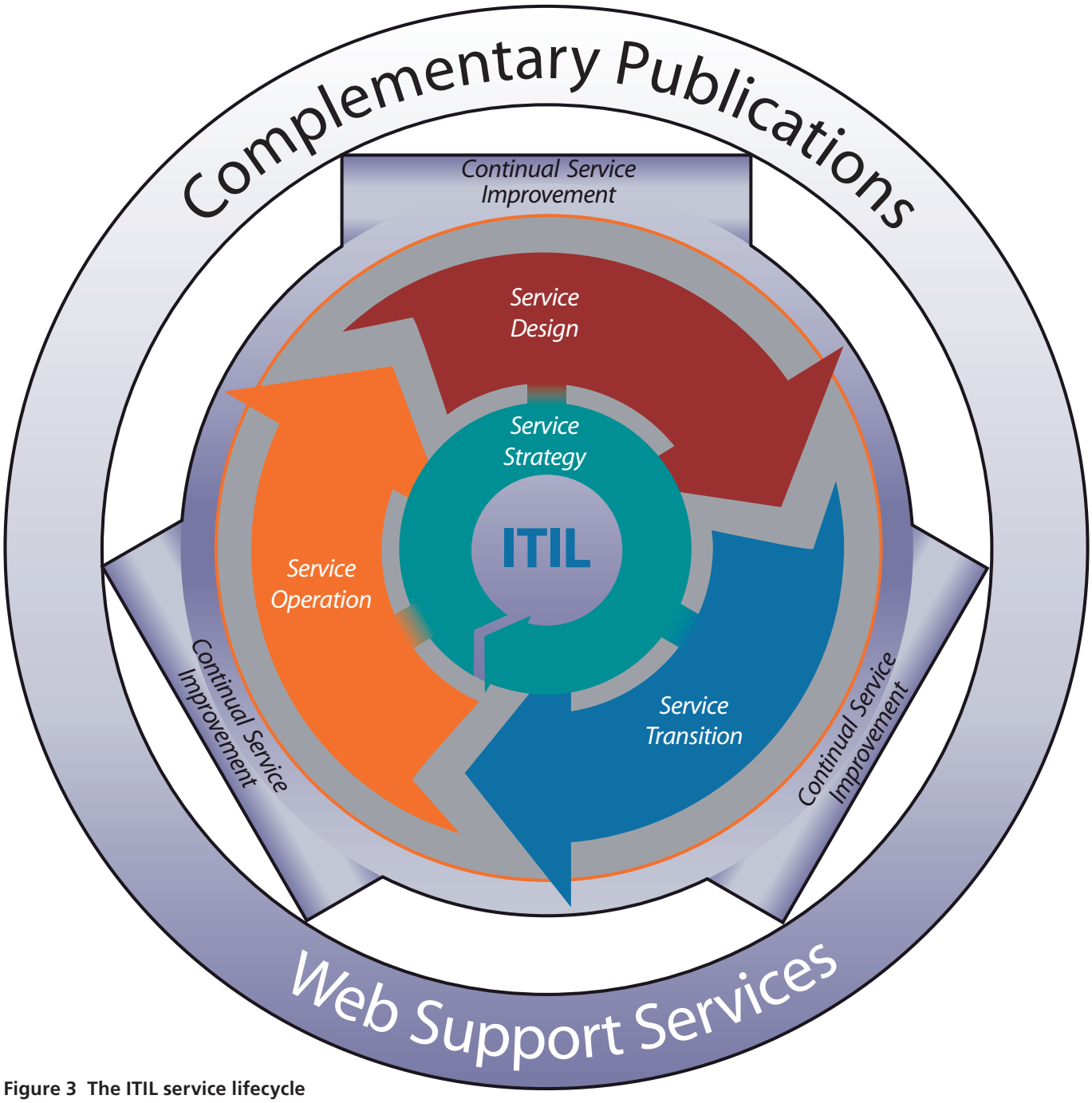

Figure 3 The ITIL service lifecycle

influence on the other and relies on the other for inputs and feedback. A constant set of checks and balances throughout the service lifecycle ensures that as business demand changes with business need, the services can adapt and respond effectively to them. The service lifecycle stages and guidance are as follows:

1. **Service strategy** establishes an overall strategy for IT services and for IT service management. It begins with understanding the organization's objectives and customer needs and how to create value for customers. Service strategy matches the service offerings to customer needs. It defines the requirements, capabilities and resources to deliver the service offerings successfully. The costs and risks associated with service delivery also need to be matched to the value delivered to the customer.
2. **Service design** covers the design principles and methods for converting strategic objectives into portfolios of services and service assets. It ensures that new and changed services are designed effectively to meet customer expectations. It includes the changes necessary to assure continuity of services, achievement of service levels, and conformance to standards and regulations. It guides organizations on how to develop capabilities for service management including the service management system, measurement method, technology and processes.
3. **Service transition** the service design is built, tested and deployed into production with minimal unwanted consequences. It covers the transition of an organization from one state to another while controlling risk and supporting organizational knowledge for decision support. It provides guidance on managing changes, release and deployment management, controlling assets and configurations, service validation and testing.
4. **Service operation** includes guidance on achieving effectiveness and efficiency in the delivery and support of operational services to ensure value for the customer, user and service provider. It provides knowledge for operations managers and practitioners to make better decisions in areas such as managing the availability of services, controlling demand, optimizing capacity utilization, scheduling of operations and avoiding or resolving service incidents and managing problems.
5. **Continual service improvement** provides guidance in measuring and improving the services to create and maintain value for customers. It combines principles, practices and methods from quality management, change management and capability improvement.

7 Conclusion

IT service providers and those managing outsourced IT have an active role to play in managing digital continuity – ensuring that the technical environment adequately supports the information assets that the organization relies on, and supports the way the organization needs to use that information after change.

To achieve this we recommend that you:

- Understand the business needs for information and its context of use
- Define information assets by content and business use rather than by the system that holds the information
- Define the scope of an IAR, design it, and use it to improve the way you manage your digital information (using existing configuration management approaches where possible)
- Use your IAR to help you to understand and record the relationship and dependencies between your information assets, business requirements and technical environment
- Use your IAR when contracting with new IT service providers, to ensure good information asset management.

In this way, information assets become true configuration items and you will be able to effectively manage and maintain digital continuity, reducing risks as the technology and the organization itself changes.

The changes we suggest you make to your IAR will enable you to collate the information you need to:

- Identify information assets that you need to use, but that are currently unsupported by the right technology and so do not meet your business requirements
- Understand the potential impact of organizational or system change
- Ensure that your enterprise architecture planning and implementation reflects how your business needs to use its information assets
- Build the long-term business requirements for information use into IT system design and development, to minimize the impact and cost of change
- Plan the migration of information assets to standardized technology and open standards wherever possible
- Identify where you can standardize your technology software, environment and formats used to minimize reliance on bespoke systems, proprietary software or complex formats. This will make your technology environment easier to manage and ensure that changes have minimal impact on digital continuity
- Identify and plan the realization of savings and efficiencies by ensuring that your technology mirrors your business requirements for information use. In particular you may be able to:

- Identify technology that is supporting unneeded information assets, allowing you to dispose of any surplus technology capacity
- Identify opportunities to downgrade the technology you use to access information or migrate it to different formats
- Move information assets to cheaper, more efficient and effective storage, avoiding duplication of assets.

You can find more information about managing digital continuity at **www.nationalarchives.gov.uk/digitalcontinuity**

Annex A Glossary of terms and definitions

asset	Any resource or capability. Assets of a service provider include anything that could contribute to the delivery of a service. Assets can be one of the following types: management, organization, process, knowledge, people, information, applications, infrastructure, and financial capital. *Source: ITIL Service Strategy* An information asset is information held by an organization, categorized from the perspective of its content and business use rather than by the IT system that holds it. Information assets could be single or logical groupings of files, data sets or databases, and include both the digital object and associated metadata. *Source: Digital Continuity Project*
digital continuity	The ability to access and use your digital information assets, in the way you need to, for as long as you need to, over time and through change. Achieving digital continuity means ensuring your information assets are complete, available and usable through the alignment of business requirements, information assets and technical environment. *Source: Digital Continuity Project*
digital obsolescence	The inability to read a digital object because the software, hardware or systems required are no longer available or are no longer supported. Digital obsolescence may result from the supplier no longer trading, having ceased support or only supporting newer versions of its products. Digital obsolescence may lead to incompatibility or lack of interoperability. The term can also be applied to specifically to hardware when it is known as technical obsolescence. *Source: Wikipedia*
digital preservation	The long-term archival management of digital information assets selected for their historical value, once they have passed out of business ownership. *Source: Digital Continuity Project* The long-term, error-free storage of digital information, with means for retrieval and interpretation, for the entire time span the information is required for. *Source: Wikipedia*

Annex B Key roles and responsibilities

Identifying the right roles and responsibilities in the organization

Ensuring effective management of information assets requires the clear allocation of responsibilities within an organization to provide:

- Strategic ownership and accountability, to secure commitment and action from the right people, to realize business benefits, to manage information risk and ensure good governance throughout the information lifecycle, and to drive a culture of effective information management
- Ongoing planning and action, and collaboration across the business, and across information management, information assurance and IT functions
- Clear business ownership of and accountability for information assets, to ensure that each one is managed in a way that is consistent with business need.

The exact shape of this framework will vary for each organization, but key roles and functions are outlined below.

Key roles in managing information assets

Senior sponsor for digital continuity champions appropriate governance and action at the right levels in the organization and across appropriate business units. The senior sponsor will be the senior business owner for digital continuity across the organization, and may be your senior information risk owner or another board member. The senior sponsor will appoint someone (for example, a 'senior responsible owner') to take forward action on digital continuity.

Senior responsible owner for digital continuity will have delegated authority from the **senior sponsor** and should have a clear route for escalating issues to board level as necessary. Who takes this role will depend on your organization; it could be your chief information officer, head of knowledge and

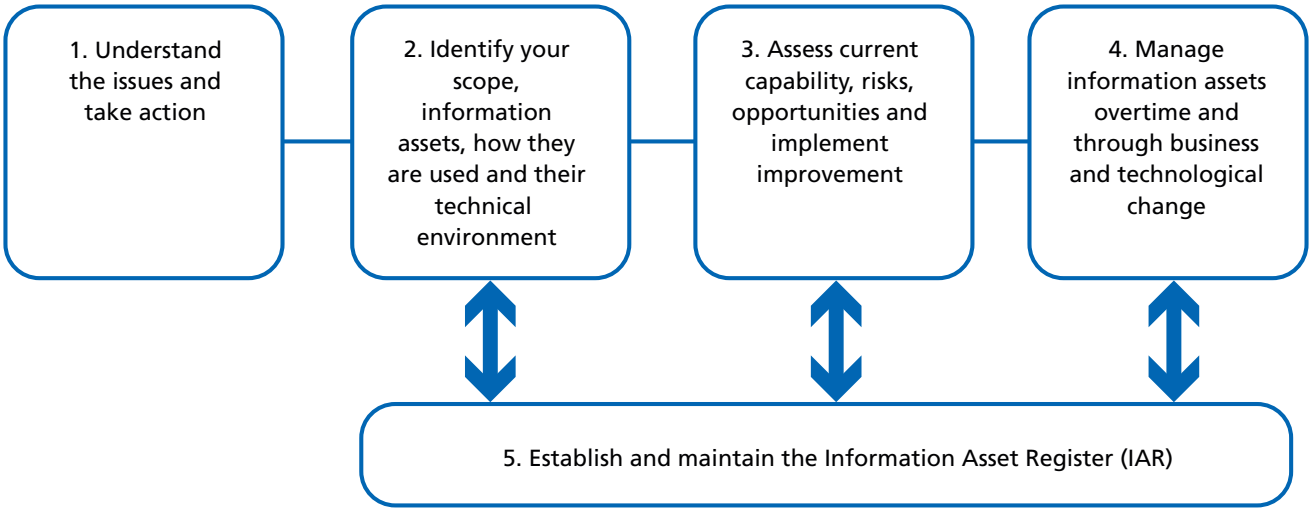

Figure 2 Key steps to improve the management of your information assets

information management, chief technology officer or another person with the remit for managing digital information, information technology or information risk.

Information asset owners *'are senior individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, who has access and why, and how it can be properly shared and exploited. As a result they are able to understand and address risks to the information, and ensure that information is fully utilised'*
UK Cabinet Office Guidance on Mandatory Roles

Functions and roles that collaborate to manage information assets

- **Knowledge, information and records managers** work with information asset owners to define how the business needs to use its information assets, now and over time, and ensure that information management supports this.
- **Information assurance specialists** ensure digital continuity is addressed as part of the spectrum of information risk.
- **IT managers** ensure the organization's technical environment enables the continuity of information assets in line with the business requirement, over time and through change.
- **Enterprise architects/strategists** ensure that enterprise architecture and/or IT strategies properly account for the ongoing business need to use information over time and through change.
- **Business change managers, project and programme managers** ensure that digital continuity is appropriately taken into account in any business change initiative, through design, implementation and test phases.
- **Procurement, commercial and contract managers** ensure that appropriate responsibility for identifying and managing continuity issues is clearly defined in supplier contracts, and that suppliers deliver on their obligations.

Annex C Managing digital continuity

The key stages shown in Figure 2, which is shown again here, provide a framework of actions your organization can take to help you assess and improve the management of your digital information assets. One of the principal ways you can manage your digital information assets is by adapting your IAR.

Step 1 Understand the issues and take action

- Ensure your corporate board and senior information risk owner are aware of the need to manage digital information assets, and understand that risk to digital continuity is a key information risk.
- Assign a senior responsible owner for managing digital information assets and their continuity.
- Ensure information technology, information assurance and information management understand their responsibilities in managing digital information assets.
- Establish a multi-disciplinary team to take action.
- Engage IT providers on the issues, and their responsibilities.
- Include managing digital continuity as a driver in relevant strategies.
- Build a business case for further action.

Step 2 Identify your scope, information assets, how they are used and their technical environment

- Identify your information assets in order to understand what information you have, and identify the business owner of each asset.
- Define how your business needs to use the information it has. Understand how each information asset will be used through its lifecycle and what value it will provide to the business.
- Understand the technical environment supporting your information assets.
- Ensure your information assets have accountable owners.
- Compile an IAR, mapping the relationships and dependencies between your business needs, information assets and the technology that supports you in using them in the way that you need to.

Step 3 Assess your current capability and implement improvements

- Identify how you will assess and manage risk to digital continuity within your existing information risk management procedures, and what additional provision might be necessary.
- Assess the organization's capability to manage digital information assets (using comparisons to international standards, ITIL and/or the CESG Information Assurance Maturity Model).
- Assess the risks to digital continuity of your current approach to managing information assets and the opportunities that would be provided by managing them more effectively.
- Create and implement a prioritized action plan to improve your information asset management.
- Improve your project management, IT service management and change management processes to assess impact on and risk to digital continuity as part of their standard procedure.
- Embed ongoing risk assessment and continual improvement.
- Identify savings and efficiencies. Dispose of the information assets and supporting IT that you do not really need and/or reduce your capability to the required level.

Step 4 Manage information assets over time, and through business and technological change

- Reflect digital continuity in business plans and enterprise architectures to ensure that you are less likely to lose digital continuity.
- Maintain a good understanding of the business use that your information assets support, so that you have the confidence to make the right decisions on what you can archive or downgrade to reduce maintenance costs.
- Assess the impact of organizational or business change on digital continuity to ensure your information assets continue to support your business needs and to avoid getting left with the cost of legacy data, costly equipment or unexpected disposal costs.
- Assess the impact of asset, business management or IT change on digital continuity and the availability of IT services to ensure your information assets continue to support your business needs and to reduce the likelihood of continuity issues arising.
- Where appropriate, aim to standardize your technical environment to make your technical environment easier to manage. Ensure that the way you manage metadata, audit data, accessibility and retrievability of information, and data quality supports digital continuity.
- Monitor and resolve incidents and problems.

Using ITIL's IT service continuity management process to manage digital continuity

This process supports business continuity management (BCM) and helps you to manage risks that could seriously affect IT services and the related information assets. It ensures that you can always provide minimum agreed service levels, by reducing the risk to an acceptable level and planning for the recovery of IT services. IT service continuity management (ITSCM) includes:

- The agreement of the scope of the ITSCM process and the policies adopted
- Business impact analysis to quantify the impact that loss of IT service would have on the business
- Risk analysis – the risk identification and risk assessment to identify potential threats to continuity and the likelihood of the threats becoming reality. This includes taking measures to manage the identified threats where cost-justified
- Production of an overall ITSCM strategy that is integrated into the BCM strategy. This is likely to include elements of risk reduction as well as selection of appropriate and comprehensive recovery options
- Production of ITSCM plans, which are integrated with the overall BCM plans
- Testing of the plans
- The ongoing operation and maintenance of the plans.

You need to consider digital continuity in your business and IT continuity management. Business impact analysis is the activity that identifies vital business functions and their dependencies. These dependencies may include suppliers, people, other business processes and IT services that are useful for the information asset register.

Annex D Bibliography and references

National Information Assurance Strategy. Available at **www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/nia_strategy.pdf**

DOD 5015.2 US Government Electronic Records Management Standard. Available at **www.defense.gov/webmasters/policy/dodd50152p.pdf**

See also *Electronic Records Management Software Applications Design Criteria Standard* available at **www.js.pentagon.mil/whs/directives/corres/pdf/501502std.pdf** and 'Records management' available at **www.en.wikipedia.org/wiki/records_management**

Governance Processes and the Management of Organisational Changes to Provide Appropriate Risk Management and Continuity Strategies. Available at **www.nationalarchives.gov.uk/digitalcontinuity**

UK Cabinet Office Guidance on Mandatory Roles. Available at **www.cabinetoffice.gov.uk/media/45149/guidance_on_mandatory_roles.pdf**

ITIL best practice information including ITIL introduction, publications, qualifications and glossary. Available at **www.itil-officialsite.com**

Acknowledgements

Authors

Shirley Lacy, ConnectSphere

Frieda Midgley, Digital Continuity Project

Judith Riley, Digital Continuity Project

Nigel Williamson, Digital Continuity Project

Acknowledgement to Digital Continuity Project

Sourced by TSO and published on **www.best-management-practice.com**

Trademarks and statements