The National Archives

Risk Assessment Handbook

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 to 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 the risks to digital continuity protects the information you need to do business. This enables you to operate transparently, accountably, legally, 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 guidance provides you with practical information and support to help you assess and manage risks to digital continuity – Stage 3 of our four-stage process of managing digital continuity. We recommend that you follow the four-stage process in order; however, you may wish to start with Stage 3.

See the diagram below for the steps in Stage 3: Assess and manage risk. This guidance covers the following steps – create a framework for managing risk (see section 3), carry out a risk assessment (section 4) and mitigate risk (section 5). For information on restoring continuity that has already been lost, see our guidance on *Managing Digital Continuity Loss*.

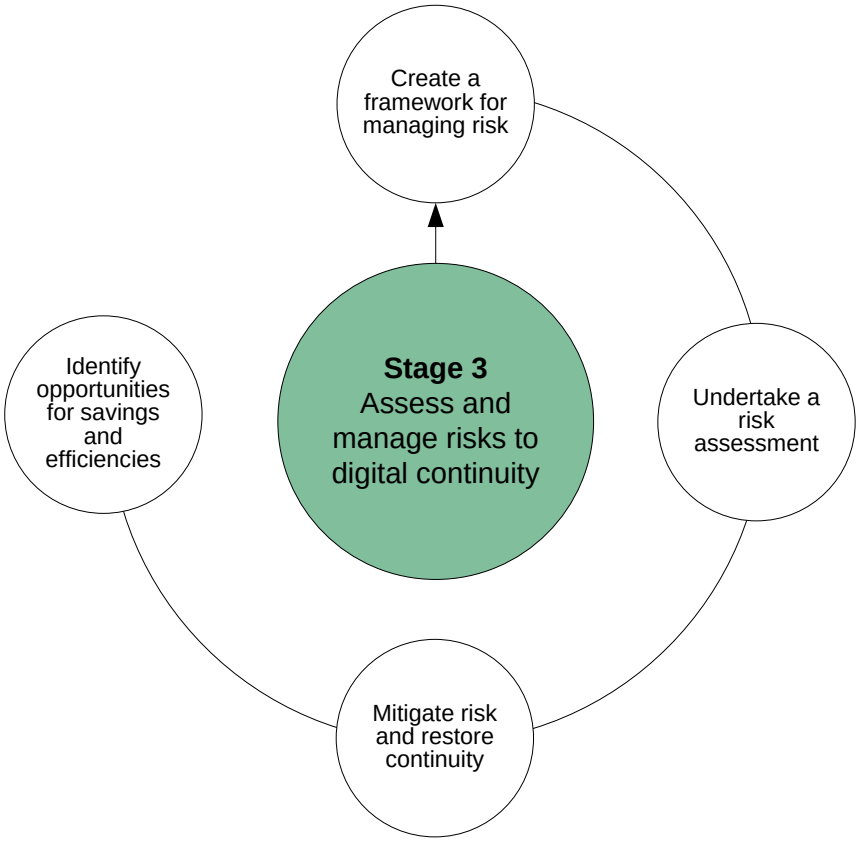

Figure 1: assess and manage risks to digital continuity

1.2 How do I use this guidance

You can use this document in two ways. For a comprehensive view of the principles and process of assessing and managing risks to digital continuity (in particular, if you are coming to this guidance without having undertaken Stages 1 and 2 of managing digital continuity), read the following sections in order.

Alternatively, the guidance can be used as a handbook to support the practical application of these principles – in this case, go directly to the section relevant to you. If you have undertaken the first stages of managing your continuity, for instance, you may want to skip to Section 4, to carry out your risk assessment.

1.3 Who is this guidance for?

This guidance is aimed at anyone involved in undertaking a digital continuity risk assessment. This could be information managers, risk managers, Information Asset Owners (IAOs) or project and change managers. As risks to digital continuity are information risks, the findings of the risk assessment will also be reported to your Chief Executive Officer (CEO) or Executive Team. For more on the people who will need to be involved in carrying out a risk assessment, see section 3.1 of this document.

See more on the roles and responsibilities that your organisation will require to ensure the digital continuity of your information in *Managing Digital Continuity*.

2 Understand risks to digital continuity

2.1 What do we mean by risks to digital continuity?

Unless you actively manage your digital information you may find yourself unable to use it in the way that you need or for as long as you need: this is a loss of digital continuity. You need to understand the factors that could cause this so that you can take appropriate measures to prevent it.

Digital information is vulnerable at times of change: this could be a single, defined change event, or the cumulative result of small changes that occur over time. Digital information is also complex – you may not fully understand what you need from your information or how these needs are met (for example, how your technology supports you in using information). This puts you at risk of a failure of digital continuity.

A failure of digital continuity will be experienced as an inability to **find**, **open**, **work with**, **understand** or **trust** your information. The causes of these failures are wide-ranging.

You may be at risk if:

- there are gaps in your information governance structures
- there are gaps in your information management policies and practice
- your change management, technology management and information management
- processes are not effectively integrated

See section 4.1 for full details of these risks to the continuity of your digital information.

2.2 Why manage risks to digital continuity

Imagine if:

- you couldn't find information for a public inquiry
- you couldn't claim emergency financial assistance because your financial data is buried in out-of-date software
- you couldn't pay pensions because you lost the metadata connecting people to the contributions they'd made
- you needed records of decisions for legal compliance, but had no way of telling if you were looking at the final version of documents

If you do not understand and manage the risks to the continuity of your digital information, you may be unable to protect your information appropriately or to exploit it fully. This will affect your ability to meet your business needs.

If you manage digital continuity, you will have confidence that the information you need to operate transparently, maintain public confidence in your organisation and protect your organisation's reputation can be found – that is, complete, in context, and trustworthy. You will be able to account for your organisation's actions and decisions.

You must ensure you manage your digital information appropriately and to an auditable standard, in line with statutory and legal requirements and best practice guidelines.

An Information Assurance Maturity Model (IAMM) was created to assist CEOs to develop an effective change programme to improve information risk management, and includes assessing and managing risks to digital continuity in line with your other information risk management procedures.

3 Establish a framework for managing risks to digital continuity

Before you carry out a risk assessment, you should establish a framework for managing risks to digital continuity. This defines the process you will follow and identifies the outcomes you wish to achieve. It will help to ensure consistency in the way your risks are identified and managed and will enable you evaluate the effectiveness of the actions you take.

To be effective, it is important that your framework is consistent (as far as possible) with the information risk management processes that are already embedded within your organisation. If you have an existing framework for managing information risk, you should extend this to include risks to digital continuity.

You also should ensure that your digital continuity risk assessment reports are available to support decision-making within your organisation.

Your digital continuity risk management framework should do the following:

- set out **roles and responsibilities** for managing risks to digital continuity
- define **objectives** and success criteria for the process
- define **the scope** of your risk assessments
- describe **the process** of how risks will be identified, analysed, controlled, recorded, monitored and reviewed
- consider how you will provide **assurance** of this process

Your framework may also address incident management.

3.1 Roles and responsibilities for the management of risk

Roles and responsibilities for managing risks to digital continuity should be clearly defined. The skills required to effectively manage digital continuity cross disciplines and the following people are likely to have some role in identifying and managing risks to digital continuity. Note that every organisation is different and roles, responsibilities and job titles may vary – so you may assign responsibilities differently in practice.

Responsivities for risks to digital continuity should be allocated to the following roles:

- Chief Executive Officer (CEO), or Executive Team
- Information Asset Owner (IAO)

- Information Management (IM), Information Assurance (IA) and Information Technology (IT) specialists
- Change or project managers
- IT suppliers or service providers

You should decide who will be involved in the risk assessment and how they will contribute. For instance, your specialists in IM, IA, IT and business change could each lead on separate areas of the assessment to give an organisational view when combined. Your CEO, Executive Team and IAOs will understand how your organisation's structures and processes support them in managing information risk. Business users and front-line staff can highlight specific concerns or issues that might not otherwise come to light.

You should ensure that staff (or external agencies) in these roles understand their responsibilities for the management of risk. You may need to provide training or guidance on what is required of them.

See Appendix A for a list of people who you may need to interview for your risk assessment.

3.2 Objectives

You should define your objectives for assessing and managing risk to digital continuity. Your own objectives will be specific to your organisation, but we have given some examples below:

- To enable you to meet the requirements of level 3 of the IAMM
- To provide you with an understanding of risks to the continuity of your digital information assets which will enable you to take properly informed decisions, in line with business objectives, on how to mitigate those risks
- To reduce the number of incidents of loss of digital continuity your organisation experiences
- To enable you to integrate digital continuity decisions into your wider information management, information assurance, information technology and change management strategies and processes
- To provide a risk report which can be used to prioritise action, including when and how to use other digital continuity guidance, tools and services
- To reduce the financial impact of losses of digital continuity on the organisation (note: this could also be to reduce reputational or operational impact)
- To reduce the impact of a specific major change event, such as a change of IT supplier, or a loss of personnel during organisational restructuring

3.3 Scope

You should determine the scope of the risk assessment, in terms of the area of the organisation to be assessed, the information to be considered and the timeframes or risk factors concerned.

Note: you may already have defined the scope for your management of digital continuity in Stage 1 of the process. If so, this will help inform the scope of your risk assessments.

Organisational unit: You can assess risk at the level of the entire organisation, an individual business unit or a specific project or activity. For government departments, the assessment may also extend to agencies or other related public bodies.

Information coverage: This will usually be all the information assets which support the activities of the organisational unit being considered. Alternatively, the scope may be limited to business-critical information, sensitive information, or information held within certain systems, managed by a particular service provider, or in specific formats or media.

Timeframe: Your risk assessment will usually consider risks which may arise over the entire lifecycle of your information assets. Remember that risks to information assets can increase over time (for example, as a result of changes to your organisation, personnel, or technology); they can also decrease (for example, as information becomes less sensitive or less critical to your business activities). It may be useful to limit the timeframe considered by the assessment to the duration of a particular project or change activity.

Risk factors: You will usually aim to conduct a comprehensive assessment; however you may decide to focus on particular risk factors, for example, your information governance structures, change management processes or technical environment. You may choose to do this because one of these areas is under review or because you believe there is a weakness in a particular area.

The level of detail of the assessment will depend upon your business needs. Looking at your objectives in carrying out the risk assessment should help you to establish the most appropriate level of detail to consider.

3.4 Process

Define your process for carrying out the risk assessment, setting out how risks will be identified, analysed, controlled, recorded, monitored and reviewed.

3.4.1 Risk identification process

When identifying risks to digital continuity, you will need information from a wide range of people, including those in the roles listed in section 3.1 above. You could approach the risk assessment in a variety of ways. You could:

- ask individuals for specific information
- hold interviews to gain a broader understanding of risks and issues
- run workshops with participants from different business areas
- choose a combination of these

The workshop approach can be particularly useful for exploring the relationships between your information and your business or how technology supports your information. It can help to highlight good practice and identify gaps, and may also prove beneficial in bringing together specialists from related fields, such as IM, IA and IT.

See Appendix A for a list of staff who may be able to contribute to your comprehensive assessment of risk to digital continuity.

You will also need to consult a range of documentation held by your organisation. For example:

- risk registers
- strategy and policy documents
- previous assessment reports
- internal audits, National Audit Office reports or other assurance reporting
- an *Information Asset Register* (IAR), or similar database, which your organisation has used to map the relationships between its information assets, business use and technological environment

See Appendix B for a checklist of documents that may help you conduct a comprehensive assessment of risk to digital continuity.

3.4.2 Risk analysis

Your framework should set out how you will analyse the risks identified during your assessment. The purpose of this analysis is to support you in making judgements about how to manage risks – it is not an exact science and it is not necessary to develop highly complex mechanisms for analysing risks to digital continuity. For example:

- Assess the probability and potential impact of each risk. The probability is the chance that the risk will occur. The impact is a measure of the consequences if it does occur. These are commonly scored on a scale of 1–5
- Combine probability and impact scores to give an overall risk priority number. This is commonly done by multiplying the two individual figures
- Assess the timeframe in which action may be required – a higher score would indicate more immediate action. Timeframe may also be factored in to your risk priority score

You should define a threshold risk priority score, above which you consider a risk to be significant. As part of defining this threshold, you will need to consider your appetite for different types of risk. If you have an existing risk management framework, risk appetite may have been determined at board level for your organisation as a whole. Alternatively, tolerances may have been set for individual projects, for example, in a Project Initiation Document.

Your risk appetite is a measure of your willingness to accept the type of risk identified (note that an organisation may be prepared to accept different levels of risk for different types of digital information). In determining your risk appetite, you should consider the following:

- What are your objectives in managing risks?
- Which types of risk require immediate action? Which can be accepted?
- What issues have arisen in the past – and what were the consequences?
- How can limited resources be best deployed to minimise risk?

Your risk analysis process will enable you to prioritise risks, escalate each risk to the appropriate level, ensure ownership at a sufficiently senior level and identify appropriate and timely action.

3.4.3 Controlling risk

Your framework should set out what actions you will consider to control risks to the continuity of your digital information. Three general categories of action may be appropriate:

Risk Mitigation

This approach focuses on reducing your risk by taking action to **decrease either the probability or the impact of the risk**. For example:

- Migrating information from an at-risk format to a standardised format would reduce the probability of continuity loss caused by format obsolescence

- Making information publicly available could reduce the operational impact of a loss of continuity of an information asset, since the information content would be recoverable from an external source (such as an internet archive)

Risk avoidance

You may be able to avoid a risk altogether, for example, by redesigning business processes to reduce reliance on at-risk information, or ceasing to hold the information asset concerned.

Risk transfer

You could consider transferring risk to a third party. For example, clarifying the contractual responsibilities of your IT service provider may reduce the financial impact of continuity loss if the provider accepts responsibility for managing and restoring continuity.

Note that while financial or contractual risks may often be effectively transferred, it is rarely possible for government organisations to transfer reputational or compliance risks.

3.4.4 Recording risk

Once you have identified risks to the digital continuity of your information, you should document these in a formal report. Wherever possible, aim to be consistent with other risk management processes used within your organisation.

You risk assessment report template should include the following:

- **Describe each risk**, including the business consequences of a loss occurring. Ensure that risks to digital continuity are also captured in other risk registers where appropriate
- **Analyse each risk** applying the scoring method defined by your framework

You may wish to include high-impact risks to digital continuity in reports to your organisation's audit committee or feed these into your organisation's overall risk improvement report to the audit committee or board. You should also explore whether digital continuity risks with high impact should be quoted in your organisation's strategic risk register.

3.4.5 Monitoring and reviewing risk

Your digital continuity risk assessment process should be iterative and responsive to change. Each risk assessment is a snapshot of the situation at the time it was carried out: over time the risks themselves, their probability of occurrence and their potential impact on the business will change.

Your framework should define how often your risk assessment reports must be reviewed to ensure that the risks identified are still current, that any new risks have been documented and that your assessments of probability and impact are still valid. We recommend you do this at least annually and when triggered by significant change events.

Your framework should define the intervals at which to repeat a full risk assessment. This should be at least every two years, or when the organisation, your information or your technical environment undergo significant change – for example, taking on new responsibilities that require information to be used and managed differently; upgrading or changing your IT systems; closing or merging projects and teams.

3.5 Assurance

You should put structures in place to provide you with assurance that the framework is being applied, and that your risk management process is effective. For example, staff training, metrics on risks and issues identified in each business area, availability of up-to-date risk registers and issue logs, use of feedback from incident analysis to refine the risk management process.

You should develop processes to ensure that the controls identified are put in place rather than simply planned.

3.6 Incident reporting and management

You are likely to identify specific incidents of loss of digital continuity during the course of your risk assessment. You should take the following actions:

- Manage the incident in line with your usual procedures for incident reporting: you should capture it in the appropriate issue logs and include it in your annual statement on internal control
- Investigate the cause of the incident. Use this information to identify other information assets that may be at risk from the same underlying factors. Document and manage this risk accordingly
- Investigate whether your risk identification and management process was effective. If not, use this information to make changes to your risk management
- Investigate whether it is desirable or possible to restore continuity: consider the value of the information to the business, the cost of restoring continuity, whether this could be achieved in a timely way, whether the information could be more cheaply or readily recreated or re-acquired from another source. Plan action accordingly

4 Carry out a digital continuity risk assessment

Once you have established a framework for managing risk to digital continuity, you will be able to conduct a risk assessment following the process you have defined, and then write a report based on your findings. This section gives you key areas to explore to help you identify where you are at risk of losing digital continuity.

4.1 Identify risks to digital continuity

To successfully manage your digital continuity, you should ensure that:

- continuity requirements are embedded within information governance structures
- continuity requirements have been defined with an understanding of what information you have, its business use and the technology required to support that use
- continuity requirements are embedded within change management processes
- information assets are managed to enable continuity requirements to be met

Examining each of these areas for gaps can help you identify where you are at risk of losing digital continuity. This section describes why these factors are important and how they can impact digital continuity.

4.1.1 Governance

Risk area	Indicators of effective management	Indicators of risk
Roles and responsibilities		
Effective management of digital continuity requires clearly defined roles and responsibilities, integrated with your wider information governance structures and policies Without these, your staff and suppliers will not have a consistent understanding of what is expected of them, will lack accountability and will be unable to ensure continuity of the information assets for which they are responsible	Your CEO has appointed a Senior Responsible Owner (SRO) for digital continuity, at the right level, and with delegated authority to act • A multi-disciplinary team has been established to take action on managing digital continuity, including skills from the IM, IT, IA and business change functions • Information Asset Owners recognise their responsibilities for maintaining digital continuity and are adequately supported in doing this • You have engaged with your IT service providers and they recognise their responsibilities for managing digital continuity. Your contractual arrangements reflect this understanding	• You do not have clearly defined roles and responsibilities for managing digital continuity • You have not appointed individuals across the organisation to take this forward • You have not made your IT service providers aware of your digital continuity requirements and have not included it in your contractual arrangements
Information management		

Engagement from your IM, IA and IT teams will help ensure that your policies support maintaining digital continuity Ensure you have well designed and implemented policies, and ensure people understand and comply with them	• Your policies support managing digital continuity. They cover: what tools to use to capture information, what information to keep and where, how to name and describe it, how to secure it, version control, use of email systems • Staff are properly trained and understand their responsibilities for managing information • Compliance with policies is high • Policies are reviewed and updated regularly to ensure that they remain effective	• Your policies do not include measures that will enable you to manage digital continuity • Staff do not understand their responsibilities for managing information • Compliance with policies is low or staff are able to opt out • Policies are monitored, policies are not reviewed and updated
Change management		
Digital continuity is at risk during change. Your requirements for using information should be integrated into your change management processes to ensure that the impact of change on your information assets is assessed and managed	• The organisation has a clearly defined change management process • Success criteria for change include maintaining digital continuity • You assess the impact of change on the continuity of your digital information assets. This is done as an integral part of the change management processes	• There is no consistent process for change management • The success criteria for change are undefined or do not include maintaining digital continuity • You do not carry out digital continuity impact assessments as an integral element of planning for change
Risk management		
Loss of digital continuity is a key information risk which must be managed in a systematic	• Loss of digital continuity is recognised as a key corporate information risk	• Loss of digital continuity is not recognised as a key corporate

and consistent way. It requires appropriate channels for risk reporting and escalation. Addressing gaps in this area will enable you to manage digital continuity, and will improve the effectiveness of your actions	• You have a framework for managing information risk • Risks to digital continuity are managed in line with your other information risks	information risk • You do not have a framework or effective process for managing information risk • Risks to digital continuity are not managed in line with your other information risks

4.1.2 Alignment of information assets, business requirements and technology

To manage digital continuity, you need to:

- know what information you have and where it is
- understand how you want to use it, now and in the future
- make sure your technology enables all this and is agile enough to meet your changing requirements

Any gaps in this understanding and alignment place you at risk of losing digital continuity, because you if do not understand your requirements for using information, you will be unable to ensure that they are met.

Risk area	Indicators of effective management	Indicators of risk
Information management		
You need a comprehensive understanding of your information assets. Without this understanding you will be unable to manage risks to your information assets Every information asset should have a defined	• You have a comprehensive register (preferably an IAR) of your information assets, covering all information of value to the business • You understand where you rely on information owned or managed by	• You hold information that is not managed as an asset • You rely on information that is owned or managed by another organisation but do not have clear processes for assuring their management of this information

owner who is responsible for understanding requirements and ensuring continuity Remember, you may be dependent on information assets that are owned, produced or managed by another organisation	third parties and have assurance that its continuity is being managed • You routinely test for continuity	
Understanding business requirements		
You need to understand what business purpose your information assets serve. Without this you will unable to ensure that you can provide the right level of support for them, enabling them to be found, opened, used, understood, and trusted as required	• You understand what information your business requires, and how it flows through the organisation • You have defined your need to find, open, work with, understand and trust each information asset, in order to meet your business needs • You have defined how long you need to retain your information	• You hold information that has no clear business use • You do not understand what information the business requires or how it flows around the organisation. • You are unsure how long you should retain your information
Technical dependencies		
The completeness and availability of your digital information is highly dependent on the technical environment that supports it Without the appropriate technology you will be unable to use your information as required to meet your business needs	• You understand your technical environment • Your technology meets your requirements to find, open, work with, understand and trust your information • You technology is sustainable and you understand how planned technical changes could affect your ability to use	• You rely on proprietary formats that can only be used with specific technology products • You rely on specialist, bespoke or legacy systems • You use file formats that are at high risk of technical obsolescence • You create information that is highly

	your information in the future	structured or has complex interdependencies, including datasets and databases

4.1.3 Business or technological change

Digital information is vulnerable at times of change. Change events can affect the alignment of your information assets, and their business requirements and technical environment, leaving you at risk. Changes may be large-scale with impact across your business or technology, but remember that small changes can also have an impact on digital continuity. For example, changes of personnel can leave you unable to find, open, work with, understand or trust your information – unless you understand and manage the risks involved.

Risk area	Indicators of effective management	Indicators of risk
Change management processes		
Successfully managing digital continuity through change requires your staff to understand and apply your change management processes	• Staff understand your change management processes and follow them • You have processes in place to manage small-scale or routine changes • Staff have the skills to conduct digital continuity impact assessments as part of planning for change • You have a process for testing for continuity following change	• Your change management processes are not well understood or followed within the organisation • Your change management processes only cover large projects • You do not have enough understanding of your information or technology to conduct meaningful impact assessments • You do not test for the continuity of information assets following change
Technology change		
Technology change may occur on an incremental basis as you upgrade your systems	• Your technology environment, including licenses and support contracts, is likely to	• You are planning to re-tender your commercial ICT services (within the next

or as the formats and software products you use become unsupported Change may also be dramatic, such as changing your IT suppliers or undertaking large-scale systems development or architecture projects Any technology change may impact your ability to find, open, work with, understand or trust one or more of your information assets	be stable for the next two years. You can't foresee any major end-of-lifecycle changes • You understand the roadmaps for the technology you use, and have plans in place to manage any transitions	two years) • You do not understand the development roadmaps for IT products you rely on • You do not have exit strategies in place for systems that are approaching the end of their life
Organisational change		
Organisational change may occur on an incremental basis as staff leave the organisation or projects come to an end Change may also be dramatic, such as a transfer of functions between organisations following Machinery of Government change	• You do not expect to undergo significant organisational change within the next two years • You understand the routine changes that will occur (staff turnover, projects beginning and end) and have processes in place to manage the continuity of your information through these transitions	• You expect to undergo a change of organisational function (such as a Machinery of Government change) • You plan to restructure the organisation or undertake an activity that will result in a loss of staff skills and knowledge and new business requirements for your information • You are aware of legislative or regulatory changes that will affect the way you record, handle, analyse or share information

4.1.4 Risks to information assets

Risk area	Indicator if effective management	Indicators of risk
Find		
Maintaining your ability to find information over time and through change relies on it being where it should be, being searchable and with appropriate access permissions If these factors are not actively managed you risk being unable to find your information when you need it. This is a failure of digital continuity	• Staff understand where to keep information. It is held in defined locations, accessible to anyone with a business need to find it • Your information has the appropriate metadata to make it discoverable by search (for example, meaningful title, subject, dates, author) • Your information is covered by your search tools. These are well-configured and usable • Your search tools return a manageable number of results, allowing the information being sought to be identified	• There are no defined locations where staff should keep information, and no defined criteria for what information should be kept • Information is held in email boxes, email archives, on local hard drives and removable media • Information is held in unmanaged network drives • Your files are not meaningfully named and do not have metadata that supports searching • Your search tools do not cover all locations where information may be held • You hold duplicate information • Your search tools are difficult to use, or staff lack the necessary training
Open		
Maintaining your ability to open information over time and through change relies on being	• Offline information can be physically retrieved in a timely and cost-effective	• Information is held on removable media such as disks or tapes

able to obtain it in a timely manner You need the correct technology and access rights. If these factors are not met you risk being unable to open your information when you need it. This is a failure of digital continuity	manner, with appropriate access controls • The integrity of your digital information is managed; you have processes to check that that your files are not corrupt • You manage access controls, passwords and encryption keys to ensure that you can open your information when required • You understand the technical dependencies of your information, and maintain the required hardware and software environment • You do not rely on bespoke, legacy or unsupported information systems. Your information is held in standardised formats with a high degree of interoperability	• You do not test for continuity regularly or following change • Staff are able to apply passwords or encrypt files as they wish. Passwords and encryption keys are not centrally managed • Staff are able to use unsupported software to create files, licences are not managed • You rely on bespoke or legacy systems which are difficult to support, or are a poor fit with your corporate infrastructure
Work with		
Maintaining your ability to work with information over time and through change relies on it being held in formats and systems that allow it to be used or re-used as you require You will also need access to the necessary	• Your information is in formats and systems that support how you need to use it (for example, information can be read, edited, saved. Data can be queried, combined, manipulated, reported on or exported as required) • You maintain the completeness of your	• Your information is siloed, it is difficult to combine, manipulate or re-purpose it • You do not understand how linked or embedded documents are used, or how your systems support these • You do not understand the range of formats you hold, or what technology is

technology or tools. Without this you risk being unable to open your information when you need it This is a failure of digital continuity	information through managing links or relationships between information. You can identify all related material and bring it together when needed, even when it is held and managed separately • You understand what tools are required to support this use, and your technology planning process ensures that they will be available	required to open and work with these
Understand		
Maintaining your ability to understand your information over time and through change relies on it being in the right place, complete and adequately described	• The information in the asset is subject to a classification scheme (e.g. a file plan) • Staff complete descriptive metadata and assign meaningful file names • You have a defined version control system that is used by all those creating and editing information within the information asset • You have a process to ensure that relationships between information are maintained	• Your information is not categorised or labelled • Your systems do not allow metadata to be assigned. Staff do not recognise the value of assigning meaningful and accurate metadata • You hold multiple versions of the same information. It is not clear which is the current or definitive version
Trust		
Maintaining your ability to trust your information relies on understanding where it came from, how and when it was used or	• You understand what audit or provenance information you need in order to trust your information. Audit	• You are unable to set or enforce access restrictions on access to your information, or staff do not understand

changed and by whom Trust also depends on knowing which version of your information is current, and on understanding data quality and accuracy The level of trust you need in your information will vary depending on what you need to do with it, e.g. information that may be used as evidence will have more rigorous trust requirements than other material	records are held and managed appropriately. You can analyse audit trails when required • You keep a record of the way information is accessed, used and changed. For example, through version control or through maintaining a record of access to information • Access rights to information are controlled • You have a forensic readiness policy and process for managing the continuity of your forensic evidence information	how and when to do this • Your access control mechanisms lack the required granularity • You are unable to audit access and use of your information or you cannot analyse audit trails • You hold multiple versions of the same information • Your information is not accurately described to indicate its purpose, source or history • You do not have processes in place to manage the continuity of audit and logging information and do not manage these data types as information assets in themselves

5 Create an action plan for mitigating risk

Once you have identified your risks and put them into a report, you should create an action plan for mitigating them.

5.1 Prioritise risks

Prioritise the risks you have identified according to their probability, impact, timeframe and whether they fall within your risk appetite. This prioritisation will enable you to identify those risks that require mitigating action.

Accept lower priority risks, but monitor them to ensure they remain within your risk appetite.

5.2 Identify options for risk control

For any particular risk to the continuity of your digital information, there may be a range of possible risk-reduction actions. These will often be focussed around reducing the probability of the risk, but may also be aimed at reducing the potential business impact, avoiding the risk or transferring it (see section 3.4.3 for more information about approaches to controlling risk).

For each risk identify the possible options and assess their probable effectiveness, along with the cost and ease of implementation. Remember, a combination of actions may be required to achieve the required degree of mitigation, and it may not be possible to mitigate the risk fully.

Identify actions which are dependent on third parties – for example, your suppliers – this may affect the cost of the action, and the degree of control you have over progress or outcomes.

In certain circumstances, you will not be able to identify appropriate or cost-effective action to control the risk, or to control it to the required extent. In this situation undertake contingency planning to enable you to respond to any issues that arise. This may include identifying measures to reduce the impact of the issue, identifying resources, or developing communications strategies.

5.3 Plan and take action

For each risk to be controlled, you should do the following:

i. **Describe the action(s) to be taken.** Document why you have selected this course of action and identify the expected outcomes.

ii. **Determine how to measure whether the desired outcome has been achieved.** Note that for successful management, both the risk and any action must be owned and approved at the appropriate level.

iii. **Assign responsibility for implementation**, allocate resources and identify timescales for action.

iv. **Monitor the progress of actions and test their effectiveness**, using the measures already identified to assist you. Remember, the probability and impact of the risk may change as actions progress: it will be necessary to reassess these and to intensify or relax mitigation measures as necessary to bring the risk within acceptable limits and keep it there.

v. **Ensure that you learn from monitoring** the effectiveness of the action you take: Which actions have proved effective in controlling each type of risk? Which types of action is your organisation good at? Where do you require additional support?

6 Next steps

Digital continuity should be embedded into your organisation's information risk policy and risk management processes. You should use the risk assessment to help you develop and maintain a schedule of risks (and mitigations) for each information asset.

You should also embed digital continuity into your change management processes. Ensure that a full assessment of the impact of change on the continuity of information assets is conducted as an integral part of your change management process.

Your assessment of risk to digital continuity should be repeated at regular intervals. As part of this process you should consider whether continuity has been maintained during the period since the previous assessment. Evaluate the effectiveness of risk-management actions, and assess new risks.

7 Further guidance

7.1 Tools and services

Your organisation may already have a range of tools, which it employs in its standard approach to risk management, to help you identify, record and manage risk. For instance, you may have standard templates for documenting risks and developing action plans. You should investigate whether you can use any of these existing tools to support your digital continuity risk assessment. Talk to your corporate management function to find out what's available.

Self-assessment tool

The National Archives has produced a digital continuity self-assessment tool to help you ask the right questions, identify areas of risk and identify possible mitigation actions.

File profiling tool

The National Archives offers a file format identification tool (DROID) which can help you understand the format, volume and ages of the information you hold – this can enable you to assess your exposure to the risk of format obsolescence. Reports generated from DROID may also help you to identify opportunities for disposing of redundant information or to identify possible mitigating actions. Find out more about DROID by consulting our guidance, DROID: user guide.

You can download our latest version of DROID for free. For previous versions go to http://droid.sourceforge.net/. For more information, see our PRONOM resource.

If you are interested in using DROID at your organisation, would like a live DROID demo, or are experiencing any problems using DROID, contact us at pronom@nationalarchives.gsi.gov.uk.

Crown Commercial Service Framework

To support your organisation's management of digital continuity, there is a range of services and solutions available on the Crown Commercial Service framework for your organisation to procure. The services available provide expertise in specific areas of information management and information technology. The solutions available cover technology to improve particular areas of the management of your digital continuity, such as data quality.

Appendix A: Interviewees

Staff in the following roles may be able to contribute to your comprehensive assessment of risk to digital continuity. Please note many of these titles are specific to central government, so where possible we have also listed alternatives if these roles don't exist in your organisation:

Chief Executive Officer or Executive Team	
Chief Information Officer (CIO)	this could be the Head of IT
Digital Continuity Senior Responsible Owner (SRO)	or someone operating at board level in your organisation who is responsible for managing digital continuity
Information Assurance Programme Manager	
Information Risk Manager	
Representative Information Asset Owners	
Head of Knowledge and Information Management (KIM)	this is Head of Information Management or Records Manager
Information Manager	
Departmental Records Officer	
Information Architect	
Information Re-use Advisor	
Freedom of Information / Compliance Advisor	
Chief Technology Officer (CTO)	or Head of IT / IT Manager
Head of Information Technology (IT)	
IT Service / Solutions Manager	or Head of IT / IT Manager
IT Business Support Analyst	
IT Procurement Manager	
IT Integration Manager	
Enterprise Architect	
Business Continuity Manager	
Business Change Manager	
Change Control Manager	

For more information on the responsibilities of those listed above, see *Managing Digital Continuity*.

Appendix B: Documentation checklist

A pre-assessment review of documentation provides an essential understanding of the department's organisation, policies and objectives. It enables the risk assessment team to define, ahead of discussion sessions, potential lines of questioning.

The document titles given below are generic. Where document titles differ or are combined within other documents, the team should use their discretion to select appropriate material for review; equally the team may wish to consider additional material to support the assessment.

File reference	Documentation	Available (yes/no)	Notes
Cross-departmental strategy and policy			
	Organisation chart		
	High-level business objectives		
Information asset management			
	Information risk management policy		
	Latest Information Risk Report to Cabinet Office		
	IAO roles and responsibilities		
	Any further internal guidance relating to the role of the IAO		
	IAR and supporting guidance as managed by the IAO		
Information management environment			
	Introduction to the organisation's information architecture		
	KIM strategy		
	Electronic records management policy		
	Electronic information classification scheme and associated retention schedules		
	Digital continuity strategy		
	Digital continuity action plan		
	Information re-use policy and supporting guidance		
Information technology environment			
	ICT strategy		
	High-level introduction to the organisation's enterprise architecture		
	Any existing mapping of the organisation's tech-environment		