# Managing Digital Obsolescence Risks

## GUIDANCE FOR SIROS

April 2009

The National Archives


**The new Version 2 of the Information Assurance Maturity Model (IAMM) contains criteria about managing the risks to information caused by digital obsolescence as one of the 'Through-Life' IA measures. This guidance will help SIROs to address these initial requirements.**

### What is the Digital Obsolescence Risk?

Digital obsolescence is the state in which digital information is no longer available and understandable for business use. Unlike paper, which can be kept on a shelf for lengthy periods, digital information is fragile and needs active intervention to survive.

Most departments have business-critical information that they need to keep for long periods such as operational records or precedents, but the business value and utility of this information can be lost if there is a failure in continuity of access to it.

Addressing the risk of digital obsolescence requires ensuring that digital information remains fit for purpose in its current technological and management environment. It is about ensuring that the information an IT system contains continues to be available and usable by the business and so retains its value.

To do this, you need to address the risks to the integrity, availability and usability of your information that specifically arise from the management of changes in technology and operational processes. SIROs should manage this like any other data handling information risk, ensuring its likelihood and impact are reduced.

### What Causes Digital Obsolescence?

The continued ability to use digital information over time is affected by changes to the technological, operational and organisational environment. Such changes can include the introduction of new applications and technology (as when existing hardware and software is superseded), changes to information management processes for capturing and managing information and metadata and machinery of government changes that redraw organisational boundaries. Examples of digital obsolescence risks include:

#### Context is Missing

When original documents survive but the information about them (metadata) is missing, the significance of the information is lost. There are examples from hospitals of x-ray records losing their value because they are no longer connected to the patient data. Even more problematic are the videos from surveillance cameras, which only have meaning if information is kept about when and where the images were captured. In these cases the **information integrity** and **authenticity** is compromised.

#### Technology is Obsolete

Simply having a robust back-up regime is not enough to ensure the long-term survival of digital information. Technology becomes obsolete, as one IT system is superseded by another, which can affect every aspect of information. For example, software used to create information can become obsolete, leaving information in formats that cannot be used with available technology and storage media can become outdated and decay. In this case, the **availability** of the information is compromised as it is no longer possible to open the information in the current technology environment

### Technology is Incompatible

Older information may have been migrated to new formats to ensure its continued availability. However, new applications and operating systems used by the organisation may not provide the same functionality as previous systems. For example, dynamic formats transferred to PDF cannot be manipulated or interpreted as intended. In this case, the **usability** of the information has been compromised.

## How Does Digital Obsolescence Relate to Information Assurance?

"Effective IA should ensure appropriate levels of ***availability***, integrity, confidentiality, non-repudiation and authentication of information and information systems."[1]

Availability of ongoing business information is a key aspect of Information Assurance (IA). IA has traditionally addressed the integrity and availability risks around data and IT systems. Addressing the risks of digital obsolescence can be understood as taking action to maintain the integrity, availability and usability of the information content for a business context. Therefore the risk of digital obsolescence should be a key feature of any organisation's IA strategy and information risk management practices.

## What Should You Do First?

In order to meet the level one requirements of the Information Assurance Maturity Model, you simply need to ensure that there is a reference to the risk of digital obsolescence in your IA Risk Register, so that the risk forms part of the information risks being managed by your organisation. This reference might say:

### 1. Risk:

Integrity, availability and usability of digital information needed by the business will be lost due to digital obsolescence and changes in the technological, operational and organisational environment over time.

### 2. Mitigating Action:

- Identify material with long term business value
- Identify the people in the organisation it impacts
- Develop a plan for its long-term survival: identify staff that need to be involved and ensure this team contacts the Digital Continuity Project to plan its next steps. Relevant staff could include Information Managers, IT, Knowledge Managers, Records Managers or Information Assurance. (In many cases you will already have a team who are liaising with the Digital Continuity project)
- Examine the list of first steps in this Guidance to help you determine what you can easily do next to begin to understand and manage your risks and move through the further levels of the IAMM

## What Should You Do Next?

The National Archives is working with all major departments on the centrally funded Digital Continuity project to enable the long-term availability of government's digital information. The project is developing a flexible shared service for central government that will include guidance, standards and a Framework of tools and services. Guidance will cover how to identify and manage information at risk of digital obsolescence, using a step by step approach. It will be published incrementally, as it is developed, at: www.nationalarchives.gov.uk/digitalcontinuity

[1] A National Information Assurance Strategy, Cabinet Office, p4.

# Appendix: First Steps towards Digital Continuity

The National Archives

To achieve level one of the Information Assurance Maturity Model, you must complete step one, outlined below:

### Step 1: Is Digital Obsolescence recognised as a potential risk in your organisation's risk management structure?

- Make sure that loss of continuity to digital information is recorded as a potential risk in your risk management structure
- Ensure there is a risk owner for Digital Obsolescence who can escalate the risks to the Board's attention if necessary

## Next steps

The steps you need to take to address the risks of Digital Obsolescence are incremental. Here are some further actions your department can take to begin to understand and manage your risks and ensure continuity of your digital information. These steps will help you progress through the levels of the Maturity Model.

### 1. Do you know who is responsible for ensuring the continuity of your information?

- Appoint a Senior Responsible Owner who has overall responsibility of ensuring that there are systems and structures in place to ensure the continuity of information over time and through change

### 2. Does your information asset register include details of information content as well as information systems?

- Undertake a technical audit so you understand the volume of data you hold, where it is, how old it is, and the range of formats it is held in. This could also allow you to understand better how quickly you are increasing the volume of data created and stored
- Use existing information management taxonomies to describe the classes of information that have ongoing value for the organisation or otherwise need to be kept. In particular, make sure you have a list of information classes that have to be kept for legal reasons, and know how long they have to be kept for
- Use the technical audit and information classes to create a comprehensive information assets register that maps your information landscape. If you do this, you will know what information you need to keep and what technology it is being kept in, as the first step towards understanding your digital obsolescence risks and mitigation requirements

### 3. Do you understand how context adds value to your business information?

- Review metadata standards – are they adequate? Are they being followed?
- Review your comprehensive information asset register and identify what contextual information is needed for the content to be interpreted and used in the future

### 4. Are you confident you can discover business critical information when you need it?

- Determine the amount of unstructured data you have and how it is managed
- Determine the level of risk to the organisation (e.g. financial, reputational) of having business-critical information in unstructured, hard to find places. This includes not being able to find information that might be the subject of legal discovery
- Determine how information flows through your organisation and what information is needed, when and by whom to support your business operations

5. When you go through system change is the information you need still available and usable in the new system?
   - Understand the technical profile of your information and what areas of your business critical information are at risk from digital obsolescence
   - Make sure you know if you have business-critical information which was created by one system but not migrated during upgrades. Ensure you know how long the supplier intends to support those legacy systems
   - Ensure adequate testing takes place on your business-critical information to check that you can continue to access and use it

6. How are you ensuring your IT suppliers are supporting the ongoing integrity, availability and usability of your information?
   - Talk to your suppliers to ensure they understand the issues and risks involved in maintaining digital continuity
   - Test supplier assertions regarding the ongoing integrity, availability and usability of your digital information over time

7. When you go through organisational change do you have contingency plans to ensure the survivability of information?
   - Draw up a plan to ensure that each information asset owner is held accountable for the stewardship and safe hand over (if any) of information assets through Machinery of Government and other organisational changes. This should include an inventory of information described by technical and business value characteristics, based on the information asset register. It should also include a report to the relevant board(s) on how these assets were retained, redistributed or disposed of

8. Is the management of your information risks balanced by business benefits?
   - Ensure there is an understanding of the benefits that can be realised through having continuity of access to the right information and that business decisions about the need to keep and use information drive risk mitigation actions
   - Ensure Information Management, Information Technology and Information Assurance are working together to support the business needs of the organisation and manage digital obsolescence risks collaboratively

## For more information

Further guidance to help you achieve these steps will be available over the next 12 months.

If you'd like to find out more about digital continuity visit www.nationalarchives.gov.uk/digitalcontinuity