



1. Q&As about digital continuity

Q What does 'digital continuity' mean?

A Digital continuity means the ability to find, access and use your digital business information for as long as you need to. In practice, that means making sure that digital information is:

- **Complete:** it's all there, and still has the metadata and links needed for the information to make sense.
- **Available:** you can find the information and open it with available technology.
- **Usable:** you can use the information in a way that meets current business needs.

Q Why is digital continuity a problem?

A There are lots of links in the chain that keeps digital information available and usable over time; at organisational, operational and technological levels. Failure to address risks in any one of these areas could cause digital information to turn from a valuable business asset into a costly liability.

Digital information is a problem because of its very nature. It is complex, involving many background processes when created, saved, opened, used or transferred that simply don't apply to paper. Digital information can be stored in lots of different places. There may be multiple copies of it – a typical PowerPoint presentation is stored at least seven times across an organisation's computer system, for example. There's a huge volume of digital data too – and more is being created at a faster rate than ever.

The media that digital information is stored on and the software used to write it can easily decay, or become obsolete as one technology is superseded by another. Expert opinion varies as to how long it is before digital obsolescence emerges as a problem, but it could be as little as five to seven years from the point of creation for some formats.



Q What are digital continuity risks?

A Digital continuity risks are those that cause digital information to become incomplete, unavailable or unusable over time. They make it difficult to find or retrieve our documents and digital files, cause loss of functionality, or prevent us from knowing if a document is authentic, for example. They can also cause separation of metadata from information, thus removing the context and rendering it useless, or costly to re-interpret.

Some risks are already well understood – network interruptions, technical failures and malicious attacks, for example. These can temporarily, or sometimes even permanently, affect the availability and use of our digital information, but they are adequately addressed by existing IT, Information Assurance or IT management processes.

Some risks are less well understood, and are not currently adequately addressed as a result. These are where risks to the completeness, availability and usability of digital information occur over time. We've identified three areas where action may be required:

- **Organisation** Examples include not properly identifying information that has ongoing business value and therefore not managing the risks to it effectively; not including digital continuity risks in your risk management processes; not really understanding what puts digital information at risk.
- **Process** Examples include not managing digital information properly (which could result in a loss of metadata); not thinking about continuity issues when negotiating IT contracts; inadequate information management processes so you don't know what you have or where it's kept; not effectively planning for the survival of information during times of change, for example when staff leave or retire, or during machinery of government changes.
- **Operational** These are risks that directly cause digital information to become



incomplete, unavailable and unusable. This includes everything from losing metadata and obsolete or incompatible hardware and software, through to inadequate management of encrypted information.

Q Does digital continuity affect my organisation or government department?

A Yes – all government departments depend on long-term access to digital information to work effectively and efficiently, operate legally and accountably, maintain public trust and improve public services. If we could no longer find, use or trust the information we have stored over time, we'd have a serious problem.

However, the risks for individual government departments are likely to be different, depending on the nature of the information you hold, what you use it for, what business and office systems you have, and the complexity of your information environment. Make sure that the potential risk of loss of continuity is clearly flagged in your departmental risk structure. This will make it easier for your department to explore and address your department's specific digital continuity risks.

Q Is digital continuity really a priority?

A Yes. Information is an asset – like cash, buildings and people. Imagine not being able to access information concerning nuclear, medical, biological, environmental and food safety, for example. We depend on digital information such as CCTV footage for national security, electronic evidence and records in the criminal justice system, and digital imaging in the border control system.

Some information is needed for a long time – you may need it to inform new policies and service development, to provide evidence to public inquiries, or answer FOI requests, for example. Not being able to find, access or use it will damage the efficient delivery of public services, your reputation and performance - it will have as serious a consequence as any



other form of data loss.

Government is taking this risk seriously. Central government departments have funded the Digital Continuity Project, managed by The National Archives. The project will deliver a Digital Continuity shared service for government that consists of guidance, standards and a Framework of tools and services. Much of the guidance, and the Framework of tools and services will be ready by the summer of 2010, with the service fully operational and embedded within The National Archives by early 2011.

Government has included the need to address continuity risks in the 2008 HM Government Guide *Managing Information Risk*. The CESG Information Assurance Maturity Model now also includes the minimum requirement that government departments add digital obsolescence risks to their risk register (CESG is the National Technical Authority for Information Assurance at GCHQ).

Q Is addressing digital continuity difficult or expensive?

A No, it doesn't have to be. The Digital Continuity project is designing a service for government that is flexible and offers real value for money, giving you considerable choice over what you spend and when.

Digital information requires active management to remain complete, usable and available over time – but the actions required are incremental, and needn't cost a lot of money. You need to recognise that digital continuity is a risk, carry out a risk assessment and prioritise mitigating actions – but we're providing guidance and support to help you at every stage, and a Framework that will help you to find the right technology or services, cost-effectively.

Taking action to address digital continuity could actually bring about efficiency benefits and cashable savings too. For example, tackling organisational and process risks now is often more cost effective than waiting until technology risks occur further down the line as data



recovery is expensive and not always possible. More effectively managing the information you need to keep and disposing of what you no longer need should save storage costs.



2. Q&As about the Digital Continuity shared service for government

Q What is the Digital Continuity project?

A The Digital Continuity project is managed by The National Archives and funded by 16 central government departments. We're developing a shared service for government to help you access your digital information for as long as you need to.

Q What is the Digital Continuity shared service?

A The Digital Continuity shared service will include guidance, standards and a Framework of tools and services, that will help you to make sure your digital information remains complete, usable and available over time:

- **Guidance** will be a central part of the Digital Continuity shared service. It will help you to understand and assess risks to your digital information and data assets, understand how to mitigate those risks and how to take effective action. We're developing guidance incrementally and will publish it on an ongoing basis on our website.
- **Standards** will define the attributes of a range of risk assessment, planning and mitigation tools, so that you can assess new tools and technologies not available via the existing Framework.
- **Tools and services** will be delivered through a Framework Agreement, procured under OJEU rules. This Framework will provide a catalogue of pre-assessed technological tools and solutions, professional information management services, and integration services that you



can draw on to address the continuity risks you've identified.

Q What do you mean by a 'shared service'?

A A shared service is something that government, and the wider public sector, can use to address a shared problem in a cost-effective way – in this case, the need to actively manage digital information to ensure its long-term survival.

The shared service we're developing won't result in a 'one size fits all' product. Instead we will deliver a flexible package of guidance, tools and services, and standards which you can use to address your specific needs. The whole package will be managed and delivered by The National Archives.

The Framework will cut the time and costs of repeated procurements across government and will provide an opportunity for enhanced value for money via agreed pricing, licence terms and aggregated purchasing.

Q Who is the Digital Continuity shared service for?

A Initially we're targeting central government departments, because they funded the project. But the service we deliver will be available to local government and the wider public sector too.

Q How can we use the Digital Continuity shared service?

A You can choose when and how to use the Digital Continuity shared service to make sure you're managing your risks. But here's how we anticipate it working:

- You'll use our guidance to set up a project team, understand your information assets and IT environments, and evaluate what's of real business value.



- You'll carry out a risk assessment – using our guidance to help you understand the specific continuity risks to your business.
- You'll develop an action plan of how best to mitigate these risks both now and in the future, again using our guidance to help you.
- You'll implement your plan, using our guidance, standards and buying appropriate tools and services from our Framework if you need them.

Q What will the Digital Continuity shared service cost?

A Using the Digital Continuity shared service needn't cost a lot of money. In fact there are some continuity risks that you will be able to address at zero or minimal cost. That's because we've designed the service to be highly flexible so that you can tailor how you use it to suit your needs and budgets. The first step is to recognise that loss of digital continuity is a risk, and carry out a risk assessment for your department. Once you know what your risks are, you may be able to address many of them using the guidance and standards we produce.

We're putting free guidance and advice on our website as we produce it. The National Archives will also provide support to central and local government through existing information management advisory services.

We're driven by the need to offer real value for money. If you decide to use tools and services from our Framework, they will be competitively priced, and offer flexible licensing terms where possible. The Framework will include tools and services from multiple providers, giving you greater choice. What's more, you won't have to go through a lengthy and expensive EU procurement, and you can be confident that products and services are assured by The National Archives.



Q When will the Digital Continuity shared service be ready?

A We're developing guidance now to help departments to assess digital continuity risks and will deliver further guidance on implementing continuity actions as the project progresses. Our full set of guidance and Framework of tools and services should be available by the second quarter of 2010, and from early 2011 the shared service should be available for all to use as part of the established teams within The National Archives.

By its very nature, digital continuity is an ongoing issue – we can't 'solve' it and walk away, because technologies change and evolve at an increasingly fast pace. What the Digital Continuity shared service can do is address today's challenges and ensure a robust process for dealing with tomorrow's. The project will look to set in place appropriate structures to ensure that the service is sustainable and updated as the operational, technological and commercial environment changes.

Q What risks are the Digital Continuity shared service addressing?

A Digital continuity risks are those that cause digital information to become incomplete, unavailable and unusable over time. The things that make it difficult to find or retrieve our documents and digital files, that cause loss of functionality, or prevent us from knowing if a document is authentic, for example, or that cause separation of metadata from information, thus rendering it useless.

Some risks are already well understood – network interruptions, technical failures and malicious attacks, for example. These can temporarily, or sometimes even permanently, affect the availability and use of our digital information, but they are adequately addressed by existing IT, Information Assurance or IT management processes and are outside the scope of the Digital Continuity shared service.

Some risks are less well understood, and are not currently adequately addressed as a result.



These are where risks to the completeness, availability and usability of digital information occur over time. We've identified three areas where action may be required:

- **Organisation** Examples include not properly identifying information that has ongoing business value and therefore not managing the risks to it effectively; not including digital continuity risks in your risk management processes; not really understanding what puts digital information at risk.
- **Process** Examples include not managing digital assets properly (which could result in a loss of metadata and links, over time); not thinking about continuity issues when negotiating supplier contracts; inadequate information management processes so you don't know what you have or where it's kept; not effectively planning for change that involves information transferring between systems or changes in information ownership, for example when staff leave or retire, or during machinery of government changes.

Operational These are risks that directly cause digital information to become incomplete, unavailable and unusable. This covers everything from losing metadata and obsolete or incompatible hardware and software, through to inadequate management of encrypted information.

Q What are the benefits of using the Digital Continuity shared service?

A The Digital Continuity shared service will enable you to:

- Understand and actively manage digital continuity risks.
- Use digital information as and when you require it.
- Understand the value of your digital information.

By managing your digital information in this way, you should be able to realise a host of additional benefits for your business:



- **Legal compliance** Access to digital information enables you to more easily to comply with Health and Safety, FOI and Data Protection legislation, for example.
- **Cost avoidance and saving** If you've protected your information, you'll lower the likelihood of incurring data recovery costs. You'll also reduce the business cost of not being able to use existing information, for example to support policy and service development, and avoid the reputational cost caused by losing digital information.
- **Support for policy making and service delivery** You can't do 'business as usual' if you don't have reliable access to the information you need for as long as you need it. Taking action to protect your digital information protects the investment you made in creating it, enhances your ability to make sound evidence-based decisions, and underpins good service delivery.
- **Accountability, accessibility and good business practice** Digital continuity actions should improve your ability to meet public and policy expectations for your auditing and accounting functions. Inquiries can happen a significant time after events; the BSE inquiry, for example, which reported in 2000, looked at government information going back to 1970.
- **Authenticity and integrity** Digital continuity actions should enable you to ensure your information is reliable – helping you to avoid reputational risks in the future. They will also enable you to ensure that information is fit for use, for example as evidence.
- **Preservation of historically valuable digital information** You have a requirement under the Public Records Act to preserve key information assets for future long-term archiving and public availability.
- **Information re-use** There is increasing emphasis on the potential reuse of government information, and on creating value by allowing information to be shared more widely.



Q How can I convince senior managers to address digital continuity risks?

A Addressing digital continuity needn't be expensive or difficult. We're providing guidance to help funding departments to put a persuasive business case together, assess digital continuity risks and plan appropriate actions. Taking action requires a series of incremental steps, rather than a substantial up-front investment of time and resources, which should make it easier for your senior managers to get started.

'Doing nothing' incurs substantial cost. Most significant is the cost to reputation if you lose essential digital information. Information is an investment, with real financial value. Data recovery or recreation is not always possible and is usually expensive; costs can range from £1,000 - £250,000 per file depending on the digital asset. A major high profile loss could cost over £5 million for a big department. Doing nothing is simply not an option for government.

Your senior managers should be aware of the requirement to address digital obsolescence that is referenced both in the CESG Information Assurance Maturity Model (the CESG is the National Technical Authority for Information Assurance at GCHQ), and the HM Government publication *Managing Information Risk*.

Q How will The National Archives help my department to take action?

A The action you need to take is incremental, starting with the need to add digital continuity risks to your organisation's risk register, and carry out a risk assessment. We'll provide advice and guidance to support you, which will include everything from a business plan template and a clear definition of digital continuity risks, through to assistance with analysing risk, drawing up an action plan, identifying appropriate actions and realising benefits. We'll share the lessons learnt more widely to support the wider public sector. Our guidance will be clear and practical, enabling you to take active, concrete steps to mitigate risk.



Q How does the Digital Continuity Shared Service fit with other initiatives from The National Archives?

A The National Archives is at the heart of information policy - setting standards and supporting innovation in information and records management across the UK. The Digital Continuity project is managed by The National Archives, and is one of its key priorities.

Digital continuity actions are also included in the Information Management Assessments carried out by The National Archives, and the guidance we produce for digital continuity will be coherent and consistent with other guidance from The National Archives.

We're working closely with The National Archives' digital preservation team to develop digital continuity standards and to enable, where possible, a smooth process for the transfer of records into the archives when it is time to do so.

Q How does digital continuity fit with wider government information initiatives?

A Digital continuity is part of the government's wider drive to effectively manage risks to information, and included in the HM Government publication *Managing Information Risk: a guide for Accounting Officers, Board members and Senior Information Risk Owners*.

Digital continuity is also recognised as an inherent part of good Information Assurance. The CESG Information Assurance Maturity Model includes the minimum requirement that government departments add digital obsolescence risks to their risk register. Higher levels of the Model now include the requirements to carry out risk assessment and implement actions. (CESG is the National Technical Authority for Information Assurance at GCHQ). We've chosen to work within an existing monitoring system to reduce the administrative burden on departments.

The Digital Continuity project reports into the Knowledge Council, which provides the



The National Archives

professional lead for knowledge and information management within the civil service. We also regularly update the Chief Technology Officers' (CTO) and Chief Information Officers' (CIO) councils.

[ends]

April 2009