



## **AN OVERVIEW OF THE BENEFITS OF ENSURING DIGITAL CONTINUITY**

<b>Project Name</b>	Digital Continuity Project
<b>DRAFT / FINAL</b>	Draft for review
<b>DATE</b>	19 November 2009

---

**This page is deliberately blank**

- 1. Introduction to this Guidance .....4**
  - 1.1 *What is this Guidance about?* ..... 4
  - 1.1 *Who is this digital continuity guidance for and how should I use it?* ..... 5
  - 1.2 *What is the context of this guidance?* ..... 5
  - 1.3 *What is the status of this guidance?* ..... 5
  - 1.4 *Digital continuity: background*..... 5
- 2. Digital Continuity benefits at a glance .....6**
  - 2.1 *Operate more efficiently*..... 6
  - 2.2 *Reduce costs* ..... 6
  - 2.3 *Operate legally, transparently and accountably*..... 6
  - 2.4 *Manage and respond positively to change* ..... 6
- 3. Benefits in detail .....7**
  - 3.1 *Reduce costs* ..... 7
    - 3.1.1 *Reduce your storage costs* .....7
    - 3.1.2 *Reduce the cost of your software and applications* ..... 8
    - 3.1.4 *Avoid costly recreation or recovery*..... 8
    - 3.1.5 *Protect your digital investment*..... 9
  - 3.2 *Operate more efficiently and effectively*..... 9
    - 3.2.1 *IT efficiency*..... 9
    - 3.2.2 *Knowledge and information management efficiency* ..... 9
    - 3.2.3 *Get the most out of your digital information* ..... 10
  - 3.3. *Operate legally, transparently and accountably*..... 11
    - 3.3.1 *Maintain public confidence and protect reputation* ..... 11
    - 3.3.2 *Improved service delivery* ..... 12
    - 3.3.3 *More informed policy making*..... 13
    - 3.3.4 *Legal compliance*..... 14
    - 3.3.5 *Accountability*..... 14
    - 3.3.6 *Preserving history and the freedom of information* ..... 15
  - 3.4 *Manage and respond positively to change* ..... 15
- 4. Next steps ..... 16**
- 5. Further reading..... 16**
  - 5.1 *Other Publications on Information and Records Management* ..... 16
- Appendix A: Aligning with wider government initiatives ..... 17**
  - 1. **Driving efficiency and joined-up government**..... 17
  - 2. **Protecting and leveraging information as an key asset**..... 18
- Appendix B: Potential departmental costs of losing data due to loss of continuity .....20**
- Appendix C: the current position and the future threat environment .....21**

## 1. Introduction to this guidance

### 1.1 What is this guidance about?

**Digital continuity is the ability to use digital information for as long as you need to, and in the way that you need to, over time and through change.**

Ensuring digital continuity requires active intervention, otherwise information can easily become unusable – a liability not an asset. But managing digital continuity should not be seen as a distinct activity, separate from what your business does now. It is not necessarily about new tools and expenditure; it is about managing digital information and business change in a way that ensures the continuity of your information, so that you can use it as you want, when you want. Digital continuity means managing risks and maximising cost effectiveness.

This is pressing because, more than ever, change will be the only constant for Government departments and the wider public sector. And it is when your business needs, technical environments and organisational structures change that you can lose the effective use of essential digital information. Ensuring digital continuity must therefore be an integral part of change management, information management, IT management and information assurance.

The National Archives is developing a service for government, and the wider public sector, that will enable you to assess your specific digital continuity risks and issues and to plan and take action. This includes a suite of practical, accessible guidance, and a commercial framework of tools and services.

This guidance outlines, at a high level, the benefits to your organisation of ensuring Digital Continuity. It looks at the ways in which digital continuity can support you in delivering services, realising efficiencies and protecting your investment in digital information, ensuring compliance and accountability, and managing information risk. It also signposts the ways in which digital continuity can support other current priorities in government.

This guidance has been produced by The National Archives' Digital Continuity project. We will supplement it as the project develops, to give you more detail on how to realise the benefits and to include case studies provided by government departments, which give examples of benefits realisation in practice.

## 1.1 Who is this digital continuity guidance for and how should I use it?

This *Overview of the Benefits of Ensuring Digital Continuity* is primarily aimed at:

- Digital Continuity Senior Responsible Owner (the person in the organisation tasked with ensuring digital continuity)
- Senior Information Risk Owners
- Chief Information Officers
- Knowledge and Information Managers
- CTOs, IT Service Managers and other IT professionals
- Information Asset Owners
- Business change managers, project and programme managers

This guidance should support you in making the business case for addressing digital continuity in your organisation and help you to explain why digital continuity is important.

## 1.2 What is the context of this guidance?

This *Overview of the Benefits of Ensuring Digital Continuity* is part of a suite of practical, accessible guidance that is being delivered as part of the Digital Continuity service for government. We are producing guidance incrementally and in consultation with central government departments. This guidance is part of the high-level, first phase, designed to give you a clear overview of the types of activity and outcomes required to ensure digital continuity. As we work more closely with departments to understand their specific risks and issues, we will produce more detailed and specific guidance. For more information visit [www.nationalarchives.gov.uk/digitalcontinuity](http://www.nationalarchives.gov.uk/digitalcontinuity)

## 1.3 What is the status of this guidance?

This is a consultation draft, and we welcome feedback to inform the next phase of guidance development. We are also keen to hear about examples of good practice and lessons learned. Please email your comments to [digitalcontinuity@nationalarchives.gsi.gov.uk](mailto:digitalcontinuity@nationalarchives.gsi.gov.uk).

## 1.4 Digital continuity: background

To understand the benefits of digital continuity, you first need to understand what we mean by it, what the impact of change is on digital continuity, and what managing digital continuity looks like in practice. You will find this information in our guidance on *Managing Digital Continuity*, which you can find at:

<http://www.nationalarchives.gov.uk/electronicrecords/digitalcontinuity/guidance-on-digital-continuity.htm>

## **2. Digital Continuity benefits at a glance**

**Managing digital continuity will enable you to:**

### **2.1 Operate more efficiently**

Better alignment of business needs, information assets and your technical environment through change means you can operate more effectively and efficiently.

### **2.2 Reduce costs**

Managing digital continuity means that you won't be paying for unused or unnecessary capacity, which could result in cost savings in:

- Storage, management and energy costs (by reducing the amount of information you hold).
- Licence costs and the cost of supporting some of your legacy IT systems (because you're not maintaining technologies that no longer support business need, where the cost of the systems are disproportionate to the value or the business benefit of the information they support).
- The cost of recreating or recovering digital assets (because you have ensured that the information you need remains fit for purpose).

### **2.3 Operate legally, transparently and accountably**

You will be confident that you're protecting the information you need to measure, demonstrate and track business performance and efficiency, and to manage risks, improve business delivery and meet your statutory obligations. Understanding and mitigating digital continuity risks will help you to avoid the significant reputational damage and costs associated with not being able to use essential information assets.

### **2.4 Manage and respond positively to change**

If you know what you want to do with your information and you have the right information asset management and technical environment to support that use, you will be in a strong position to respond positively to change. You will also be better able to manage the risks that change brings.

### **3. Benefits in detail**

**This section of the guidance gives you more detail about the benefits you can realise through managing digital continuity. Further supporting evidence can be found in our appendices and suggested further reading. You may find this information useful when building your business case to undertake a digital continuity risk assessment in your organisation.**

#### **3.1 Reduce costs**

Managing digital continuity means that you could avoid paying for unused or unnecessary capacity, which could result in opportunities for cost reduction or cost avoidance as the examples below highlight.

##### **3.1.1 Reduce your storage costs**

The proliferation of digital information and declining unit costs of digital storage means that organisations often opt to store everything, including storing information that is not required for business purposes. Although the unit cost of raw storage is falling, high volumes of managed digital storage bring higher costs and operational overheads.

By taking action to achieve digital continuity you will identify the digital information assets you have and develop your understanding of their value. This will enable you to take informed decisions about disposing of information that you don't need (for example through retention schedules and disposal policies).

Reducing the amount of digital information you hold unnecessarily will make it easier to manage and easier for you to prioritise cost-effective action to maintain its continuity. In turn, reducing your storage volume (for example by using de-duplication technologies, or deciding to archive using cheaper storage such as tape) means lower costs for the storage and management of your digital information. You may currently be locked into a contract which might make it difficult to realise savings in the short term, however reducing your data volumes may alleviate some potential costs of change during the contract term and/or will make it cheaper at time of re-contract. Reduced storage will also mean:

- Reduced back-up costs and time
- Reduced electricity costs
- Reduced need for physical space
- Reduced number of servers

And, of course, these actions also help to deliver your Green IT objectives.

### **3.1.2 Reduce the cost of your software and applications**

To ensure digital continuity you will need to develop a detailed understanding of your technical environment. This will give you the ability to make evidence-based, cost-saving decisions.

The process of ensuring digital continuity may enable you to identify and standardise the applications and software used in your organisation. This could reduce both your IT costs and your operational costs, as less complexity means that your technical environment will be easier and cheaper to maintain.

For example, you may be able to streamline the applications and software that you use, or identify legacy systems that are no longer required. You may also be able to use alternative, more cost-effective, software that is appropriate for the business utility you require from your information. The process of managing digital continuity may also enable you to reduce your software license and support costs as you ensure that you're only paying for licence and support that you actually need. Conversely, of course, it will help you to identify the legacy and proprietary systems that you do need, so that you can make sure they are properly resourced.

### **3.1.3 Reduce the costs of finding your information**

Large volumes of data are not only expensive to maintain, but are also more expensive to retrieve information from. It is harder to keep a track of what you've got, and to make sure you've kept the metadata you'll need to easily find it. One recent estimate for industry is that the cost of searching through digital information, for example for a public enquiry, can range from £600,000 to £1.7 million per terabyte of data held.<sup>1</sup> By reducing the amount of digital information that you hold you may be able to reduce the financial implications and amount of time spent retrieving information.

### **3.1.4 Avoid costly recreation or recovery**

The recovery of digital information is not always possible; where it is possible, the associated costs can be high. These costs can range from £1,000 to £250,000 per file depending on the complexity of the digital asset (see appendix B).

By managing digital continuity you are taking active steps to ensure that you can find, trust and use your digital information as you need to, over time and through change.

### **3.1.5 Protect your digital investment**

It costs public money to create information and we have a duty to protect that investment. If you cannot find or access your digital information assets, or they are not fit for purpose, you may have to redo work or duplicate the effort originally invested. This wastes money and resource.

In a study of US government and education workers published in February 2009, 38 per cent of respondents said that they have had to redo reports or other work.<sup>2</sup>

## **3.2 Operate more efficiently and effectively**

Digital continuity is at the heart of operational efficiency. Quite simply, you cannot operate efficiently if you can't use your digital information for as long as you need to.

Ensuring digital continuity requires the close alignment of business needs, information assets and your technical environment. This drives efficiency and effectiveness as the examples below highlight.

### **3.2.1 IT efficiency**

The [HM Treasury Operational Efficiency Programme](#) [OEP], published in April 2009, puts an emphasis on government departments realising savings through making operational processes more efficient and cost-effective.<sup>3</sup>

The process of managing digital continuity can help you to deliver IT efficiencies. That's because digital continuity requires you to align your technical environment and your information management with the utility you need from your information, over time and through change.

This process will enable you to identify areas where:

- You are providing unnecessary support.
- You have unused capability.

### **3.2.2 Knowledge and information management efficiency**

Digital continuity is efficient and effective information management in a digital age.

---

<sup>1</sup> John Merryman, Glasshouse Technologies, May 2008

<sup>2</sup> Xerox press release. February 2009

<sup>3</sup> [HMT Operational Efficiency Programme](#) April 2009

Ensuring digital continuity supports other facets of good information management, for example the need to understand what information you've got, where it is, and what value it has. Digital continuity should therefore help to deliver all of the benefits you expect from good information management. Some of the benefits you could realise through managing digital continuity are:

- Information is easier to manage and find if you can reduce your data volumes.
- Less resource and management is required to ensure that your digital information assets support your business needs.
- You waste less time and resources looking for or trying to retrieve the information that you require if you know what digital information assets you hold.
- You will have the policies and practices in place to ensure information is usable over time and through change, for example capturing and maintaining appropriate metadata.
- An organisational culture that values information and recognises personal responsibilities for safeguarding it can be encouraged by bringing together a cross-disciplinary team to assess and address digital continuity issues.

### **3.2.3 Get the most out of your digital information**

Public sector information is a valuable asset and a publicly funded resource. It is in the interest of the public, as well as your organisation, that you can realise the maximum value from it, and that information assets are not wasted.

The *Power of Information* review outlines the significant potential of the re-use of public sector information,<sup>4</sup> including its important role in the economy. In 2007 it reported that public sector information brings direct revenues to government of around £340 million; however this represents only a fraction of the value that this information creates in the wider economy. It is estimated that the Ordnance Survey alone underpins £100 billion per year of economic activity in the UK.<sup>5</sup>

If your digital information can be reused widely for as long as required, you can ensure that you get the maximum value from your information, benefiting from the initial investment many times over.

---

<sup>4</sup> "Computers allow public sector information to be re-used and combined to make new services that were never envisaged when the information was originally collected". [The Power of Information](#) June 2007 p11

<sup>5</sup> Report for Ordnance Survey, quoted in [The Power of Information](#)

Working digitally has immense benefits; you can quickly find, copy, reuse, share, import and fully utilise required information, maximising the potential for you to work efficiently through exploiting the value of your information. Managing digital continuity facilitates the operational efficiency of individual organisations by supporting re-use, also supporting the sharing of information between organisations and enabling information to be made widely available.

### **3.3. Operate legally, transparently and accountably**

Ensuring digital continuity means that you will be confident that you're protecting the information you need to measure, demonstrate and track business performance and efficiency, and to manage risks, improve business delivery and meet your statutory obligations. Understanding and mitigating digital continuity risks will help you to avoid the significant reputational damage and costs associated with not being able to use essential information assets. It will also support your information assurance, addressing a serious, but not widely recognised, information risk – being unable to use information over time and through change. Here are some examples in more detail:

#### **3.3.1 Maintain public confidence and protect reputation**

Confidence in a public sector organisation can be significantly affected if it is not able to fully account for its actions and decisions – and being able to confidently use digital information that has maintained its integrity and provenance is essential to guarantee accountability and transparency. Public sector organisations have an obligation to remain open to future public or parliamentary scrutiny

For example, if the provenance of digital information that has informed important policy decisions cannot be verified, or its authenticity cannot be definitively ascertained, the legitimacy of the decisions based on this information could be challenged. This could potentially undermine public confidence in your organisation.

Moreover, an inquiry may require access to records going back years or decades. For example, the BSE Inquiry that reported in 2000 looked at government information going back to 1970. It is unlikely that, 30 years from now, an enquiry into an event happening today would be able to access all the digital information that it required unless action had been taken to protect the continuity of the digital information assets.

[Losing digital continuity has consequences: a case study from Japan](#)

Digital continuity failure can result in information loss that can seriously damage your reputation, as highlighted by the following case study.

In 2007, the Japanese Government faced a crisis sparked by poor record-keeping in the Social Insurance Agency. One factor contributing to the problem was the introduction in 1997 of a new system to integrate multiple pension numbers into one single number for each person. However, the records were not properly maintained and handled, and by 2007, 50 million pension records couldn't be linked to the individuals who had been making payments.

The Parliamentary session due to end in July 2007 had to be extended to rush through laws to reform the Department involved, a bill to abolish the statute of limitations on pensions and a further bill to reform the civil service.

The Government had to attempt to match the 50 million unattributed pension records against the payment records of 100 million people – the entire population of those paying into the pension system or receiving payments. It had also to guarantee that everyone who made pension contributions will receive the pension due to them.

In January 2008, the new Prime Minister announced, 'The careless management of public documents, such as pension records, is absolutely unacceptable. We will conduct a fundamental review for managing administrative records and will consider their legislation, and furthermore, we will improve the system for preserving public records, including expanding the national archives system.'

Managing digital continuity will help you to make sure you can use the digital information that you need to protect reputation, over time and through change.

### **3.3.2 Improved service delivery**

Planning and delivering public services can be adversely affected if you are not able to find, access, use and trust the information that you require. This is recognised in the [Lord](#)

[Chancellor's Code of Practice under section 46 of the Freedom of Information Act 2000](#)<sup>6</sup> and [Data Handling Review](#).<sup>7</sup>

As well as protecting you against this risk, managing digital continuity can also enable the more efficient and effective delivery of public services.

To illustrate this, it may be useful to consider the future need for information about foot and mouth disease:

For example, in the event of future outbreaks, the ability to deliver information to the public is imperative. In order to make evidence-based decisions about actions to take to prevent the spread of the disease, access to statistical data and information relating to previous outbreaks will be important. If information about previous trends and contingencies were incomplete, for example because it had been saved in a format that is now unsupported by your current technical environment, any emergency planning to cope with a new outbreak may not be able to utilise this vital data.

### **3.3.3 More informed policy making**

In order to make effective service and policy decisions, you need to be confident that the information on which you are basing your decisions is authentic, verifiable and stands up to scrutiny.

Ensuring digital continuity involves ensuring essential information is complete – for example, it has the metadata you need to understand it and links to external files are still there. This supports your timely access to information which is authoritative and maintained to an appropriate standard, available in appropriate formats and with the necessary contextual information. It enables you to take sound, evidence-based decisions with confidence.

---

<sup>6</sup> Records are “the basis on which decisions are made, services provided and policies developed and communicated.” [FOI Section 46 Code of Practice](#). Of course, this could be applied to all types of digital information, not just records.

<sup>7</sup> “The failure to make the right information available at the right time can have an adverse impact on public services” [Data Handling Review](#)

### 3.3.4 Legal compliance

You have a duty to manage your digital information appropriately and to an auditable standard, in-line with legal requirements<sup>8</sup> and best practice guidelines.<sup>9</sup> There could be repercussions, such as a section 46 assessment, if reliable, verifiable information is not made available to the public or for an inquiry as and when required.

Your obligations to look after information may include:

- information about employees and members of the general public, which is covered by the [Data Protection Act](#)
- statutory responsibilities relating to specific types of records, such as the [Public Record Act 1958](#)
- information subject to the [Freedom of Information Act 2000](#) (according to the revised [FOI Section 46 Code of Practice](#) which governs your responsibility to produce information requested under the Act)

The [National Information Assurance Strategy](#) also requires government to ensure its information is protected and available as needed and the supporting [Information Assurance Maturity Model](#) includes loss of digital continuity as a serious information risk to be managed. This means that public sector bodies must consider the ongoing use of digital information as part of their information assurance strategy. If you do not, you are placing yourself at risk of contravening your legal responsibilities.

The [FOI Section 46 Code of Practice](#) outlines your responsibility to ensure that your records remain usable for as long as they are required. Requests for information made under the Freedom of Information Act 2000 may happen many years after the information has been produced.

### 3.3.5 Accountability

*'Authorities should know what records they hold and where they are, **and should ensure that they remain usable for as long as they are required**'*

---

<sup>8</sup> Legal governance relating to digital information includes; Freedom of Information Act 2000, Data Protection Act 1998, Environmental Information Regulations 2004, Public Records Act 1958

<sup>9</sup> Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000 <http://www.justice.gov.uk/guidance/docs/foi-section46-code-of-practice.pdf>

Lord Chancellor's Code of Practice on the management of records issued under the Freedom of Information Act 2000.

Information created by the public sector is central to the wellbeing, safety and rights of the population. It includes everything from medical records and police information through to legal records and citizenship documentation.

In order to ensure that your organisation remains accountable, you need to make sure that your digital information can be found, complete and in context and that its authenticity can be verified. You also need to ensure that your digital information remains open to future public or parliamentary scrutiny, which can take place many years after events.

### **3.3.6 Preserving history and the freedom of information**

Public sector information is a publicly funded resource. It can be requested by the public under the Freedom of Information Act 2000 [FOI] and is a record of our history. Government also has a duty to manage its information appropriately under the [Public Record Act 1958](#) [PRA]. If our digital information cannot be found, accessed or trusted, how will we, and future generations, be able to understand and analyse important contemporary and historical events? Access to verifiable digital information is essential if we are to avoid periods of our history becoming lost in a digital dark age.

## **3.4 Manage and respond positively to change**

Change – whether it's to your supplier contracts or a machinery of government change – is inevitable. When your business needs, technical environments and organisational structures change you're at risk of losing the use of essential digital information.

Ensuring digital continuity is critical to effective change management. For example, if you know what you want to do with your information and you have the right assets and technical environment to support that use, you will be in a strong position to respond positively to change. You will also be more able to manage the risks that change brings, and put processes and policies in place to managing change with confidence.

## 4. Next steps

The actions we suggest you take to ensure digital continuity are outlined in our *Managing Digital Continuity* guidance, which you can find at:

<http://www.nationalarchives.gov.uk/electronicrecords/digitalcontinuity/guidance-on-digital-continuity.htm>

This guidance should help you to take step one, which is to position your department to act.

## 5. Further reading

Having read this guidance, you may also find it useful to refer to:

### 5.1 Other Publications on Information and Records Management

[Information Assurance Maturity Model](#)

[National Information Assurance Strategy](#)

[The Lord Chancellor's Code of Practice on the Management of Records](#)

## Appendix A: Aligning with wider government initiatives

Managing digital continuity will support government in meeting the requirements of several wider government agendas.

### 1. Driving efficiency and joined-up government

- **Transformational government** - using IT to deliver services to the citizen efficiently and effectively, and promoting shared services and collaborative procurements.  
[http://www.cabinetoffice.gov.uk/cio/transformational\\_government.aspx](http://www.cabinetoffice.gov.uk/cio/transformational_government.aspx)
- **The HM Treasury Operational Efficiency Programme (OEP)** - published in April 2009, this emphasises the need for government to realise savings by making operational processes more efficient and cost-effective. Addressing digital continuity will help to realise these goals. It will give you a thorough understanding of your digital information assets, the environment in which they operate and how your businesses need to use them. This understanding, supported by the digital continuity service, may enable you to increase efficiency, avoid and reduce costs.  
[http://www.hm-treasury.gov.uk/vfm\\_operational\\_efficiency.htm](http://www.hm-treasury.gov.uk/vfm_operational_efficiency.htm)
- **Collaborative purchasing** - this is set out in Transforming Government Procurement, and given further impetus in the Procurement part of the Operational Efficiency Programme. Government and the wider public sector can realise strategic and cost benefits from collaborative purchasing of commonly required goods and services - and to do so we need to challenge bespoke or special requirement that increase costs and reduce market competitiveness.  
[http://www.hm-treasury.gov.uk/d/oep\\_collaborative\\_procurement\\_pu731.pdf](http://www.hm-treasury.gov.uk/d/oep_collaborative_procurement_pu731.pdf)
- **Government IT strategy** - the Operational Efficiency Programme and [Digital Britain](#) signal an evolution in the government's IT strategy, using the principles of sharing and reuse. This points to greater application re-use and collaborative procurement of increasingly standardised desktop, network and datacentre services.  
[http://www.culture.gov.uk/what\\_we\\_do/broadcasting/5631.aspx](http://www.culture.gov.uk/what_we_do/broadcasting/5631.aspx)
- **Green IT agenda** - promotes sustainable IT, including the reduction of inefficient hardware usage and power usage amongst its targets. Digital continuity should

enable you to reduce the amount of digital information you hold - which could support this move to greener IT.

[http://www.cabinetoffice.gov.uk/media/141533/greening\\_gov\\_ict080724.pdf](http://www.cabinetoffice.gov.uk/media/141533/greening_gov_ict080724.pdf)

## 2. Protecting and leveraging information as an key asset

- **[Information Matters](#)**: building government's capability in managing knowledge and information - this new knowledge and information management strategy is helping government departments seize the opportunities and meet the challenges of the digital era. The strategy sets out the actions needed for government to improve the way we manage information as a valuable asset and establishes it as a key priority for government.

<http://www.nationalarchives.gov.uk/services/publications/default.htm>

**[Power of Information](#)** - the Power of Information taskforce is working to realise the potential for reusing public information to improve public service outcomes and create new businesses. Maintaining digital continuity directly supports this agenda as it can ensure that information is managed in a way that maximises re-use potential. As a consequence, digital continuity also supports government's [Open Source, Open standards and Re-use action Plan](#) and making public data public, part of the [Digital Engagement](#) strategy

[http://www.cabinetoffice.gov.uk/reports/power\\_of\\_information.aspx](http://www.cabinetoffice.gov.uk/reports/power_of_information.aspx)

[http://www.cabinetoffice.gov.uk/government\\_it/open\\_source.aspx](http://www.cabinetoffice.gov.uk/government_it/open_source.aspx)

<http://blogs.cabinetoffice.gov.uk/digitalengagement/>

- **[Section 46 Code of Practice](#)** - the revised Freedom of Information Section 46 Code of Practice includes the obligation to ensure essential digital information remains fit for purpose, stating: 'Authorities should put in place a strategy for their continued maintenance designed to ensure that information remains intact, reliable and usable for as long as it is required.' Digital continuity will support government to do this so that its information can support effective public accountability.

<http://www.justice.gov.uk/guidance/foi-guidance-codes-practice.htm>

- **[The National Information Assurance strategy](#)** - this requires government to ensure its information is protected and available as needed - an outcome supported by digital

continuity. The [Information Assurance Maturity Model and Assessment Framework](#) includes loss of continuity as a serious information risk to be managed.

[http://www.cabinetoffice.gov.uk/ogcio/isa/publications/ia\\_strategy.aspx](http://www.cabinetoffice.gov.uk/ogcio/isa/publications/ia_strategy.aspx)

[http://www.cesg.gov.uk/products\\_services/iacs/iamm/index.shtml](http://www.cesg.gov.uk/products_services/iacs/iamm/index.shtml)

## Appendix B: Potential departmental costs of losing data due to loss of continuity

<p><b>Expenditure (per department where risk is realised):</b></p> <p><b>£5.8m:</b></p> <ul style="list-style-type: none"> <li>▪ <b>£5m</b> minimum cost of recovering lost data for a single department</li> <li>▪ <b>£225,000</b> minimum value of data lost to a single department</li> <li>▪ <b>£575,000m</b> cost of reputational damage to a single department resulting from loss of continuity (<b>£9.3m for government as a whole</b>)</li> </ul>	<p><b>Assumptions:</b></p> <ul style="list-style-type: none"> <li>▪ As a result of loss of continuity there will be at least one major, high profile information loss in one central government department over a 5 year period, resulting in the cost of expert recovery of some data and the irretrievable loss of other data, and the cost of reputational damage including the cost of unplanned and enforced cross-Whitehall activity post-event to put preventative measures in place.</li> <li>▪ The data needing and able to be recovered would be equivalent to 5000 files (based on an assumption that 0.1% of a departments' 5000 business users lose 20% of their data i.e. 1000 files each of 5 users)</li> <li>▪ Recovery costs can vary from £1000 to £250,000 per file<sup>10</sup>; the lowest estimate is used in this calculation;</li> <li>▪ The amount of irretrievable data would be the same as the amount recovered, i.e. 5000 files;</li> <li>▪ The minimum value of lost data is expressed as the average hourly FEC of an HEO (£80,000 p.a. divided by 1776 hours = £45) multiplied by an average time taken to create one file: 1 hour, multiplied by the number of files lost: 5000 = £225,000;</li> <li>▪ The cost of reputational damage is expressed as: the additional single departmental costs of senior staff time, business change and other responsive actions over a 6 month period, resulting from public or parliamentary pressure to take action to prevent an occurrence: 50% of FEC of SMS: £125,000, plus business change project costs: (5 average FEC staff for 6 months: 5 x 80,000 / 2 = £200,000; plus other project costs of £250,000); the whole multiplied by 16 (the number of central government departments who have funded the digital continuity project); plus the single departmental cost of managing a consequent additional scrutiny (e.g. PAC/select committee enquiry/NAO audit): FEC of 2 x Principal for 6 months: £100,000;</li> <li>▪ <b>The aggregate risk of reputational damage to government as a whole cannot be quantified in monetary terms, but will be high</b></li> </ul>
--	--

<sup>10</sup> Based on quotes and supplier feedback to the Digital Continuity project.

## Appendix C: the current position and the future threat environment

Ensuring digital continuity brings considerable benefits and efficiencies to your organisation, but you may encounter the argument that digital continuity loss has yet to be experienced. This appendix should help you to understand the current position for most central government departments, and the future potential risk environment.

### 1. The current position

Although there are anecdotal examples, loss of continuity has not yet proved a major or public problem for government or the wider public sector. This is because:

- There is no burning platform (yet). Historically our inability to find or use reliable information has had few consequences: e.g. the resulting loss of efficiency is usually unmeasured and therefore hidden. The likelihood is that loss of, or inability to find or rely on information will be significant only in relation to a crisis or high-profile event e.g. a public enquiry, legal discovery, or in relation to the need to discover critical information/data to measure business efficiency (e.g. historical performance data).
- We don't know exactly what we've got or exactly where it is: Which means we don't know what utility we might have lost. Although information assets are now registered as part of the information assurance process, their descriptions are high level and mainly refer to IT systems rather than the information they contain. We don't have a coherent view of what the information assets themselves are, and where they are.
- We don't know what's of value: We do not understand the value or utility of the information we hold in any way which is useful to the business, and we do not have any current means of determining this. Without an idea of utility we cannot measure the impact of loss of continuity.

### 2. The future threat environment

The risk of significant, and therefore public, loss of continuity is however likely to increase because of:

- The exponential rise in the volume of digital information held: We don't have accurate data on how much information we hold, or which our service provider holds for us.

Recent work<sup>11</sup> commissioned by The National Archives indicates central government data holdings are rising exponentially, and further significant growth in volume is likely<sup>12</sup>. Aside from the cost issue (environment and management rather than unit storage costs), rising volumes mean greater difficulties in maintaining oversight and control. In addition to volume, loss of control is also related to the increasing complexity of how information is stored, within and outside networks, in governed (e.g. EDRM) and ungoverned (e.g. personal folder) spaces, and inside collaborative interfaces (e.g. Web 2.0 applications). Loss of oversight and control particularly through organisational and other changes is a major risk to continuity.

- The increasing complexity of digital information: Due to increased reliance on born-digital objects like CAD drawings, databases, new media like Wikis, images and video. New ways of working, for example with collaborative technology tools, will themselves constitute part of the information we will need to keep. None of these dynamic forms can be kept like paper, or even like electronic paper (e.g. Pdfs) and will need a highly correlated technical environment to survive through change and over time.
- We will be more likely to notice information loss: because it is generally higher on the government and political agenda due to the information security agenda. And to the extent that the information sharing agenda grows, and appropriate re-use tools improve, the utility of older information will be more realisable. That means we'll want to revisit it more, and the loss of its utility will be much more visible. Finally the increased drive towards data evidence-driven efficiency improvements will increase the importance of being able to find, access and use reliable historical data and information.
- Our business continuity, and back-up processes and systems, only address external threats: Duplicating digital records simply duplicates the continuity risks – it doesn't address them. Operating systems, platforms and software, including EDRM systems, have no current capability to address the specific issues of technical change and obsolescence.

---

<sup>11</sup> Kable report for The National Archives, May 2009

<sup>12</sup> 2008 research by Forrester Research for Clearpace suggests industry enterprise data volume is growing by 50% annually;

- Other Governments have identified continuity as a major threat The USA, Australia, Canada and New Zealand and the EU (as well as academia) are all investing in major programmes to address digital preservation, although their focus is currently archival. The UK government has set up the digital continuity project to deliver a shared service to central government to help it achieve and maintain digital continuity across its operational business information.

[ends]

Published November 2009 in draft for review