



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information is stored on and the software used to write it can easily decay, or become obsolete as one technology is superseded by another.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.



The National Archives
