

An introduction to digital continuity

THE DIGITAL CONTINUITY PROJECT

June 2009



The National Archives



If there's a public inquiry will we be able to find the files and emails we're asked for?

digital information matters

This fact sheet explains what we mean by digital continuity, why it's important for government and the wider public sector and what we are doing to ensure government's digital information remains usable for as long as it is needed

We live in an information age

In this high-tech, digital age we're creating more information than ever before. Just think about the documents you create and need to do your job, the emails you send and receive, and the websites you refer to.

In fact, information is one of the most important assets an organisation has.

Managed well, it helps you to make sound decisions and deliver evidence-based policy; operate legally and accountably; respond to enquiries and inquiries; share learning and work collaboratively; maximise the economic value of information re-use; and support business continuity.

Managed poorly, there can be serious business, legal, financial and personal consequences.

Digital information is more vulnerable than paper

An efficient and effective government needs to be able to find, trust and use its digital information, regardless of when it was created. But surprisingly, the information you keep digitally is more vulnerable than information on paper.

You may not be able to use it when you need to because of technological change. The lifespan of a piece of digital information can be as little as five years, for example. After this time, hardware and software can fall out of use, or the media information is stored on deteriorates. Just think about floppy disks and vhs tapes.

Essential business information can easily become unreadable and unrecoverable if the technology available does not allow you to use your information as you need to.

But it isn't just technology changes that cause information to become unusable.

If your organisation doesn't have a policy that ensures the right metadata is captured at creation, and maintained over time, for example, you can easily lose information's context. In practice that might mean you may not be able to tell if you're looking at the final version, or who made critical amendments – and if you can't trust the information you have, you may not be able to use it as you need to.

Or you may not be looking after information properly simply because you don't know what you've got, or what its real value is.

Loss of digital continuity needs to be addressed as an integral part of good IT management, information assurance management and information management.

Digital continuity means taking action to keep information usable

Digital continuity is about making sure you can use valuable digital information for as long as you need to. That may sound obvious, but without action, it won't happen. You need to fully understand your existing digital assets, and ensure you have the right policies, procedures and technology for the future.

However, digital continuity isn't about keeping all of the digital information you create over time. It's about safeguarding digital information that has ongoing value for your business.

Why it matters

Without access to the information you need when you need it, you'd struggle to deliver good public services. You'd fail to operate accountably and transparently, meet legal and statutory obligations, answer parliamentary questions, or respond to inquiries. In a worst case scenario, not having the information you need could seriously damage your reputation and public trust and cause you to incur significant cost.

The Digital Continuity shared service

In July 2007, The National Archives received funding from central government departments to develop a shared service that will help government keep essential business information usable for as long as necessary. It set up the Digital Continuity project, which is delivering a digital continuity shared service. This service will be made up of:

Guidance: to help government understand and assess risks to its digital information, understand how to take effective action to mitigate risks and resolve digital continuity issues.

Tools and services: available through a Framework agreement, with a catalogue of pre-assessed technological tools and solutions, professional information management services, integration services and data management solutions that could not only support continuity but also lead to direct, cashable savings through improved information management.

Standards: to define the attributes of a range of risk assessment, planning and

mitigation tools, so that any organisation can assess new tools and technologies as they become available.

Timescales

Much of the guidance and the Framework of tools and services will be ready by the summer of 2010. The service will be fully embedded within The National Archives by early 2011.

Although initially targeting central government departments, the service should benefit the whole of the public sector. If we haven't answered your questions about digital continuity, email digital.continuity@nationalarchives.gov.uk and we'll get back to you as soon as we can.

