

Update for government

DIGITAL CONTINUITY

June 2009



The National Archives

We're developing a digital continuity service for government that will enable it to use its digital information for as long as it needs to. This will include guidance, technical tools and services, and standards.

This monthly update focuses on the risk assessment process we're developing. Please circulate as appropriate.

Simon Lovett: 020 8392 5350

Risk assessments

We're asking our 'first wave' departments to take four sequential steps:

- 1) Position your department to respond to risk.
- 2) Identify risks.
- 3) Plan to deal with them.
- 4) Take appropriate action.

Most of you have undertaken step 1 through your engagement with us so far. To enable step 2 we're developing a simple risk assessment process which we'll guide you through.

We're piloting this with DfID and the Home Office. It uses a mixture of interviews and workshops with senior departmental managers, information management and

IT staff and business users over a couple of days.

What they look at:

Corporate-level risk: strategic and organisational factors that can result in loss of digital continuity.

Business-level risk: how IT and IM systems or processes can fail to ensure continuity of information assets through change.

User-level risks: how individual technical or operational factors can lead directly to loss of continuity.

The assessment also relies on information we'll be asking you to provide through a *technical environment audit* – of what file formats, desktop and enterprise applications, databases and file storage systems you have. We need this to understand your technical risks and to ensure we get the right tools and services for the Framework we are developing.

What happens next

After an assessment we'll produce a report, private to your department. This will identify current continuity issues and future risks, and make recommendations, focusing on low resource/high

impact mitigating actions. We'll then work with you to agree priorities for appropriate action (step 3), including on how to use the digital continuity service when it is established.

Timelines

At the end of July we'll brief first wave departments further on the risk assessment process. Meanwhile we'll contact first wave departments individually to agree tentative dates for a departmental risk assessment between September and next March. We'll do the same with the other government funding departments by March 2011.

What else?

We're developing an **information management value tool** to help you identify cash and other benefits of changing the way you manage information – more next issue.

We're also developing further **guidance**: see www.nationalarchives.gov.uk/digitalcontinuity

And we're working with BuyingSolutions on an autumn procurement for the **Framework**, aiming that this will be in place next summer and available through the BuyingSolutions catalogue.