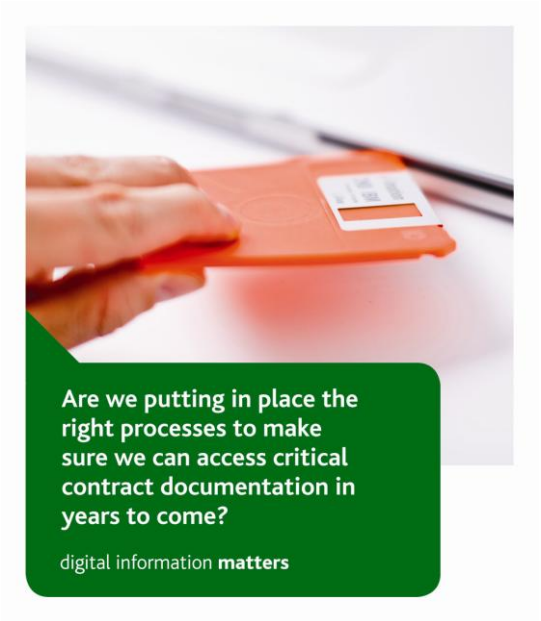
The National Archives

Assess risks to digital continuity



Digital continuity is the ability to use your information in the way that you need, for as long as you need.

If you lose digital continuity that means your digital information is not usable in the way that your business needs it to be. The consequences can be as serious as for any other information loss.

Loss of digital continuity can interrupt service delivery and incur additional cost and effort. Without usable digital information, the public sector cannot work efficiently, accountably or transparently. It cannot meet its legal or statutory obligations.

Risks to digital continuity

Digital information is vulnerable at times of change, including technical, organisational and business change. These risks can increase over time if not managed from the outset.

The impact of losing digital continuity is:

- you can't **find** the information you need
- you can't **open** the information you need
- you can't **use** or work with your information in the way you need
- you don't **understand** what your information is and what it's about
- you don't **trust** your information and can't be confident it is what you say it is.

Assess risks to digital continuity

Assessing risks is part of a four stage process for managing digital continuity. We recommend that you:

- read our Risk Assessment Handbook
- use our self assessment tool
- check for continuity using our *Testing for Continuity Checklist.*

Risk Assessment Handbook

Our *Risk Assessment Handbook* guides you through the risk assessment process. In brief, it recommends the following:

1. Create a framework for managing risk

- Define process and outcomes; clarify roles and responsibilities, objectives, scope and assurance measures.

2. Risk assessment

During your risk assessment you need to check that:

- continuity requirements are embedded into your governance structures
- they've been defined with an understanding of what information you have, its business use, and the technical environment required to support that use
- they're embedded in change management
- your information management and technical management processes protect digital continuity.

Gaps in any of these areas indicate an area of risk.

3. Create an action plan

- prioritise risks according to their probability, impact, timeframe and whether they fall within your risk appetite
- identify options for risk control, bearing in mind effectiveness, cost and ease of implementation
- plan and take action.

We recommend that you carry out risk assessments regularly – your requirements will change over time, and this may change your risk profile.

Self-assessment tool

We have built a self-assessment tool so you can assess your organisation's risks.

The tool has three sections:

1. Understanding digital continuity and roles and responsibilities.
2. Information requirements and technical dependencies.
3. Management.

Your answers to each section build a report that gives an assessment of your risk and includes suggested mitigating actions.

Download the self assessment tool from: nationalarchives.gov.uk/dc-riskassessment.

We're also developing a tool that will help you to assess the risks associated with individual information assets.

Testing for Continuity Checklist

Our *Testing for Continuity Checklist* helps you test whether your information asset meets your usability requirements. It forms part of the guidance produced to support stage three of our managing digital continuity process: assess and manage risks to digital continuity.

The Digital Continuity Service

You can use The National Archives' Digital Continuity Service to mitigate risks to digital continuity. The service is free to use by anyone in the public sector and is available from: nationalarchives.gov.uk/digitalcontinuity