Information Asset Owners and digital continuity

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

Loss of digital continuity is a serious information risk – one that you need to manage in your role as an Information Asset Owner (IAO). Without usable information, you cannot operate transparently, legally or accountably.

This factsheet gives an overview of what you need to do, points you to guidance and tools that can help you, and to people you can work with to manage digital continuity.

What loss of digital continuity means

- 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 that it is what you say it is.

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.

Your role in managing digital continuity

As an IAO, your role is about providing assurance and making sure that action is taken to manage the digital continuity of your information assets.

That's largely about understanding and coordinating the activities of others in your organisation who have specialist areas of responsibility. Your IT and information management and information assurance functions are key contacts in supporting you to manage digital continuity.

For more detailed guidance on your role, including your digital continuity responsibilities, read *The Role of the Information Asset Owner: a Practical Guide*, available here: nationalarchives.gov.uk/documents/information-management/role-of-the-iao.pdf

Ensuring the digital continuity of your assets

Managing digital continuity means making sure that your information is complete, available and therefore usable for your business needs.

To ensure the digital continuity of your information assets, take the following actions:

1. Identify your information assets

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

To assess whether something is an information asset, ask the following questions:

- Does it have a value to the organisation?
- Will it cost money to re-acquire the information? Would there be legal, reputational or financial repercussions if you couldn't produce the information on request?
- Would it have an effect on operational efficiency if you could not access the information easily? Would there be consequences of not having this information?
- Is there a risk associated with the information? Is there a risk of losing the information? A risk that the information is not accurate? A risk that someone may try to tamper with it? A risk arising from inappropriate disclosure?
- Does the group of information have a specific content?
- Do you understand what it is and what it is for?
- Does it include all the context associated with the information?
- Does the information have a manageable lifecycle? Were all the components created for a common purpose? Will they be disposed of in the same way and according to the same rules?

2. Identify how you need to use your information

You need to determine the use you need from your information assets. This covers everything from how you find it, through how you access it and what you do with it. You need to assess what your requirements are now, and how they might change over time.

The usability you need to maintain for your information over time and through change is the core of digital continuity. If you lose the ability to find, access, use, understand and trust your information in the way that you need, you have lost its digital continuity.

3. Document the relationships between business requirements and information assets

Keep a record of what you've learned. For each asset make sure the business requirements they meet, and the additional information which is vital to managing them are recorded. Your organisation may already have some form of Information Asset Register (IAR) that you can use as a starting point, adding additional fields as required.

For more detailed guidance on points one, two and three, read *Identifying Information Assets and Business Requirements*, available from: nationalarchives.gov.uk/documents/information-management/identify-information-assets.pdf

You can also download an IAR template from: nationalarchives.gov.uk/documents/information-management/iar_template.xls

4. Ensure action is taken to manage the digital continuity of your assets

Discuss how you need to find, access, understand, work with and trust your information assets with your IT, information management and information assurance teams. They can then make sure that their processes and practices support that use now, over time and through change.

Document the actions and processes you've agreed, and monitor compliance. This should form part of your report to your Senior Information Risk Owner.

You need to be confident that actions are being taken to manage the risks to the digital continuity of your information assets. You can undertake a risk assessment on the information assets that you are responsible for by using our free self-assessment tool, available from: nationalarchives.gov.uk/documents/information-management/iar_template.xls

You need to be particularly vigilant before, during and after organisational or technical change – to ensure that the continuity of vital information assets is included at the outset. Again your role is largely as an advocate, ensuring that your IT, information assurance and information management teams include loss of digital continuity as a risk, and manage it accordingly.

Use our *Testing for Continuity Checklist* to check the continuity of your information assets after change: nationalarchives.gov.uk/documents/information-management/testing-for-continuity-checklist.pdf

You might also find it useful to read:

- *Change Management for Digital Continuity SROs:* nationalarchives.gov.uk/documents/information-management/change-management-for-sro.pdf
- *Digital Continuity for Change Managers*:: nationalarchives.gov.uk/documents/information-management/digital-continuity-for-change-managers.pdf
- *Migrating Information between EDRMS*: nationalarchives.gov.uk/documents/information-management/edrms.pdf

Help from the Digital Continuity Service

You can use The National Archives' Digital Continuity Service to help you understand and manage digital continuity.

The service includes guidance, a framework of technical tools and services, a self-assessment risk assessment process, and a free file profiling tool called DROID, which will tell you what files you've got, their format, size and last modified date.

The Digital Continuity Service is available from: www.nationalarchives.gov.uk/digitalcontinuity