The National Archives

Managing Digital Continuity Loss

This guidance relates to:

Stage 1: Plan for action

Stage 2: Define your digital continuity requirements

Stage 3: Assess and address risks to digital continuity

Stage 4: Maintain digital continuity

This guidance should be read before you start to manage digital continuity. The full suite of guidance is available on The National Archives' website.

Contents

1 Introduction

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

Digital continuity enables you to operate accountably, legally, effectively and efficiently. It helps you to protect your reputation, make informed decisions, avoid and reduce costs, and deliver better public services. If you lose digital continuity and your information is no longer usable, the consequences can be as serious as those of any other information loss.

1.1 What is the purpose of this guidance?

This guidance forms part of a suite of guidance that The National Archives has delivered as part of a digital continuity service for government, in consultation with central government departments.

Digital continuity loss is experienced in five ways – you can't **find**, **open**, **work with**, **understand** or **trust** the information you have. If you are dealing with a continuity loss the big question you are asking is: 'how do I deal with the problem I have now?' But it's just as important to ask: 'how did this happen and how can I avoid it happening again?' The aim of this piece of guidance is to help you answer these questions.

Depending on the type of digital continuity failure and the type of information affected, there are a number of possible actions you can take to restore continuity. However sometimes restoration is not possible, or it is too time consuming or expensive to be a realistic option for your organisation. In these situations, it is particularly important to take action to make sure this type of loss does not happen again.

1.2 Who is this guidance for?

This guidance is aimed at anyone who has experienced a digital continuity loss and wants to understand why and how that loss happened, how they can resolve the problem and how they might avoid it happening again. This may be an Information Asset Owner (IAO) or user investigating a specific isolated loss, or it may be an information manager or Digital Continuity Senior Responsibility Owner (SRO) looking at more systematic digital continuity failures across an organisation.

See more on the roles and responsibilities that your organisation will require to ensure the digital continuity of your information in *Managing Digital Continuity*.

1.3 How to use this guidance

Knowing how to manage digital continuity losses is a component of the final stage of the Managing Digital Continuity four-stage process and you should therefore understand these previous stages. *Understanding Digital Continuity* and *Managing Digital Continuity* provide more information.

This guidance will take you through the four stages you should work through for any digital continuity loss incident:

- Understanding the digital continuity loss
- Understanding why the loss happened
- Restoring continuity (if possible)
- Preventing the loss happening again

Ideally, your organisation will have an incident management process which covers information issues generally and digital continuity specifically. This process may require you to formally record the incident in logs and lessons learned documentation and will have procedures for escalation of issues.

All incidents of digital continuity loss should be reported to the Digital Continuity SRO, who may then escalate the issue to the Chief Executive Officer (CEO), Executive Team, or equivalent. You should work alongside your Information Management team and whoever is responsible for incident management to make sure digital continuity losses are reported and escalated appropriately.

2 Understanding the digital continuity loss

You have digital continuity if your information is complete, available, and therefore usable in the way that you need it to be. If you have a failure of completeness, or a failure of availability, that means your information is not usable and you have lost your digital continuity.

USABLE = AVAILABLE + COMPLETE

USABLE: your information meets your requirements for how you want to use your information.

AVAILABLE: you can **find** what you need and you have the technology to **open** it and work with it in the way you need.

COMPLETE: everything you need to **work with**, **understand** and **trust** the information is present, including the content, context and all the necessary metadata

What constitutes 'usable' will depend on the way your business needs to use each piece of information. This may change over time. Digital continuity is about maintaining usability over time. It is lost when what you can do with the information no longer matches what your business needs to be able to do with it.

The testing for continuity checklist (see the Appendix) can be used to diagnose the particular type of failure you are experiencing, breaking each of these five issues down into further detail. You may have lost usability in a number of different ways at the same time. This may only become apparent once you have investigated further. For example, your initial issue is that you cannot find a piece of information, but when you finally obtain it, you then find that it is also un-openable.

3 Understanding why the loss happens

This is not about assigning blame for the loss, but understanding why the loss happened so you can better manage this specific incident and make plans to avoid similar problems. The root cause of continuity failures is seldom simple, often being the result of several seemingly minor oversights, or being the end result of issues with policies or training.

Understanding why and how the loss happened may actually reveal that your information never had continuity to start with; it is not that it was lost over time or through change, but that information was created or transferred to your department without that ability to find, open, work with, understand or trust it. In these situations it is often impossible to restore continuity.

Reasons why the loss happened can be broadly grouped into the following categories:

- the information management processes and procedures are insufficient
- the technology doesn't support the necessary usability
- user error – staff lack the necessary skills or knowledge, or do not follow procedures
- information transfer – continuity is lost when the information is migrated

For example: You experience loss of digital continuity because your information is stored in a file format that you cannot open.

Understanding why the loss happened is more complicated. This type of loss could occur for any one of the four main reasons described above, e.g.

- your organisation does not have a list of approved file formats, so users do not know which formats they should be creating information in, or accepting into the organisation via transfers
- the format was created by a bespoke piece of software which is no longer supported by your organisation. The replacement software can't open the old format, or can only open it with limited functionality
- the user creating the file selected a non-standard format from the options presented by the software they were using, and support for that format is not widespread in your organisation
- the information was transferred to your organisation from a third party who has a technology environment which supports the file format, but your organisation does not

For the above example, we will assume the digital continuity loss occurred due to the second reason, the retirement of the bespoke piece of software (i.e. because the technology no longer supports the information appropriately). This could have happened for a variety of reasons:

- When the system was migrated no one thought to make sure the old file types were supported
- Some files were migrated from the old format to a new format, but this file was missed in the migration process
- Your IT team did not understand what information was business critical, and how it needed to be used to support the business

3.1 Information management failure

Information must be managed and protected to support its ongoing use requirements. The information management processes and practices of your organisation should support this. Failures can occur when:

- the procedures do not cover the particular information and/or usability requirements
- the procedures are not well understood and therefore not followed
- the procedures are not easy to follow, or not seen as suitable so people deliberately do not follow them

3.2 Technology fails to support usability

Your technical environment enables you to use the information in the way your business needs. If the technology changes or your usability requirements change, this balance can become misaligned and the technical environment is no longer able to deliver the support the information requires. Digital continuity loss can occur when:

- The technical environment changes, for example:
    - a piece of technology fails – for example, a hard drive failure, or data corruption
    - support for a bespoke piece of technology has been removed
    - the information relies on legacy technology which is no longer supported
    - a piece of technology has been upgraded and it does not support the information created using the old version
    - a piece of technology has been removed before all the information was migrated – for example, removal of floppy disk drives

- The usability requirements change to something the technology environment cannot support, for example:
    - additional people require use of software with a limited number of licenses
    - additional audit trails must be applied to information which the file management system cannot record
    - information which was originally 'read only' must now be editable

3.3 User error

All the technology and processes can be in place, but there is always a human factor involved, either deliberately or accidentally people often fail to correctly follow the processes set in place. This can be due to:

- lack of awareness of the technology available or the procedures that should be followed
- lack of training in how to use the technology or how to implement procedures to their full capabilities
- knowledge is lost as staff change – either the skills required to use and maintain technology, or the knowledge relating to the information itself
- deliberate failure to implement procedures – for example, because they are onerous, or the technology is too difficult to use and staff seek alternative methods and workarounds

3.4 Information migration

Like any other resource, information is often moved around, entering and leaving organisations, and being moved around within them. If you do not manage the migration carefully, you may lose vital usability.

- Format/software misalignment – if information is transferred into an organisation from another, the new organisation may not have the software necessary to open the information with the usability it requires
- Relationship management – as information is moved around, the relationships between different pieces of information can be lost, the connection between information and its metadata can also be disconnected

4 Restoring your continuity

Your ability to restore continuity will depend on a number of factors:

- the type(s) of continuity loss experienced
- the type of information the loss has occurred to
- the value of the information to the business – the amount of resource you are willing to commit
- how soon the business needs to be able to use its information again

The way these factors combine will dictate your ability to restore your continuity and **unfortunately many situations will present combinations of these factors that mean it is not actually viable to do this**. Some types of loss are intrinsically very hard to recover from; other types of loss involve expensive restoration or will take longer than is practical. You may have to reduce your usability requirements – accepting lower quality or less functionality.

Available restoration options can be broadly grouped together into four categories, see sections 4.1-4.4 below.

4.1 Manual restoration

You may be able to restore the continuity of your information by investing in extra resources – either time or people. The suitability of these solutions will of course depend on the time and resource you have available, but can often be the simplest solution. You can consider the following options:

- manually search locations that may not be covered by search tools
- re-create the information, e.g. re-type a document that you only have a printed copy of
- re-establish the history of a piece of information by searching alternate sources, e.g. email histories or updating links and references
- find alternative versions of the information – e.g. versions stored on websites, archives, or in email. Other organisations with whom you have previously shared the information may also be able to provide a usable version

4.2 Support and training

Another member of staff may be able to restore continuity for an individual, either because they have access to different tools (e.g. to convert the format – see section 4.4 on format conversion below) or because they have additional skills (e.g. to use advanced search techniques). It may be that this person could train the user at the same time – for instance, show them how the search works.

If there is a widespread lack of knowledge or skills in how to use these tools, it may be an opportunity to do wider training (see section 5.3 below).

4.3 Extending the technical environment

If your technical environment does not deliver the usability you require, you can add new tools or services to the environment to fill in the gaps. The possibilities include:

- installing new software or hardware, including viewer, emulation and virtualisation technology
- re-purchasing old technology to allow you to open legacy formats
- purchasing or re-establishing support contracts
- purchasing additional licenses
- establishing central availability of hardware (e.g. a machine that can read floppy drives and transfer the information to a network drive)
- hiring additional resource with specific skills to manage bespoke pieces of technology

4.4 Using tools and services

You may be able to use tools and services to change the information you hold to deliver the usability you require. These tools and services could either be purchased so they become a part of your technology environment, or may be available as a service provided by an external agency or contractor who would manage the tool for you. These options can be expensive and you should follow the relevant procurement procedures.

File format conversion: You can convert the file format of your information, either to one which your organisation already supports or to one for which supporting technology is more readily available.

Content analysis tools, such as eDiscovery, can help you to find information, identify related information and provide appropriate audit trails.

Data quality tools are available to help make sure that data is accurate, this could include, database schema and data value analysis, data cleansing and master data management.

Data migration: These types of service concern moving data between one database and another. This is useful in maintaining access to your data, ensuring that it is not in databases that are isolated.

Data recovery: If your information is stored on media which you cannot read, experts in data recovery may be able to restore it. This could include files trapped due to hardware failures, but also restoring files from obscure legacy media formats.

Metadata extraction tools: These enable you to obtain technical information from the metadata embedded inside files, databases or other systems. These tools can be used to scan large systems, or individual files.

Example of the obscure file format (continued): Your ability to restore continuity will depend on what the file format is, what your business needs are, how much time and resource you are prepared to spend, and what your lead times are for the information affected.

For example, you might be able to reinstall the original software, either to enable converting the information to a different file format, or longer term to continue using the information in its original format. However this may not be possible – the software may not be available or your technology environment may no longer support it. There may also be time and cost issues of finding the software, installing it and licensing it.

You may be able to migrate the information to a newer file format using a different piece of software – but you may lose functionality or metadata along the way, which may mean the information is still not usable to meet your business needs.

5 Preventing the loss happening again

The final step of managing a digital continuity loss incident is to take action to prevent such a loss happening again. This becomes particularly important if you can't restore continuity at all – either because it is impractical, too expensive or too time consuming. Specific incidents of loss can be used to support requests for additional support and resources to manage.

Your current digital continuity loss may actually only be one example of a number of losses that have occurred across your information but have not yet come to light. You should test any information which may be susceptible to the same loss – for example be of a similar age, using similar technology or having similar usability requirements – to check whether it has lost its continuity (see our checklist in the Appendix). You should also risk assess your information to see where it is at risk of losing its digital continuity – this will help you prioritise your resources and actions to protect the information most at risk.

The actions you need to take will depend on the type of loss, the structure of your organisation and the resources you have available. The actions that you can take will broadly correspond to the reason you lost continuity (see section 3).

5.1 Information management failure

If the procedures are not suitable for all of your information, or users are not following the procedures, then you need to review your information management and improve it and the communications and training of it. If your procedures are seen as prohibitively difficult or time intensive to follow, you need to find a way to either simplify them, or better communicate their importance.

The failure may highlight the need for new policies, or updates to existing ones. For example, your organisation may have a list of supported file formats which needs to be re-aligned with technology, or a metadata policy that needs to be updated. DROID can be used to understand the file formats that your organisation is using and highlight areas of concerns.

Government is moving toward using open format standards to create and share information. You should ensure your list of supported formats is in line with those agenda.

5.2 Technology fails to support usability

You can take very specific, immediate actions to identify other pieces of information which may have lost – or be at risk of losing – their digital continuity in a similar way. For example:

- If there was a problem with a specific file format, you can use file identification tools to find and identify files of the same format
- If a particular piece of hardware failed you can test similar pieces, or start replacing them (for instance if a particular brand of hard drive failed)
- If the search tools are not able to deliver the expected results, changes could be made to the indexing or advanced options

On a larger scale, to prevent losses of continuity relating to technology happening, it is vital that you understand the individual components of the environment and how they each support the information and its usability. This mapping will enable not only better incident management, speeding up the process of identifying the impacts of a technology failure, but will improve forward planning (migrating away from formats/technologies before they become legacy) and can even drive efficiencies (removing technology that is no longer necessary).

Understanding the usability requirements of your information, the technology environment and how everything interconnects is stage 2 of managing your digital continuity and is covered by National Archives guidance: *Identifying Information Assets and Business Requirements* and *Mapping the Technical Dependencies of Information Assets*.

Once you understand this relationship, you will be better placed to manage your information and technology to prevent losses happening. See our guidance on *Embedding Digital Continuity in your IT Environment* and *Embedding Digital Continuity in Information Management*.

5.3 User error

The key mitigation to risks around staff issues is training – educating staff so that they both understand the importance of managing digital continuity and are empowered to use the tools and technologies available to them correctly. You should include this training for all new members of the organisation, but also deliver it regularly to existing staff.

There may be follow-on improvements that the technology and information management teams can make. If staff require a lot of training to use a particular tool or follow a procedure, it may be an indication that the tools can be simplified, maybe simply through improving help files or minor language changes on buttons.

Knowledge management should be reviewed to make sure that vital skills and knowledge are not concentrated in individuals. Documenting and sharing of knowledge and skills should be a standard, and knowledge transfer should be a key element of any staff exit processes.

5.4 Change management

Information management should be involved in any major changes which impact the usability of information, whether that is the transfer of information, major business change that impacts the use required of information or technology change that may affect the support of the information.

There are two pieces of guidance on managing digital continuity through change: *Digital Continuity for Change Managers,* aimed at people managing the change, and *Change Management for Digital Continuity SROs,* for those responsible for implementing digital continuity across the organisation.

Example of the obscure file format (continued): You could take immediate action to identify other files which may be in the unsupported format. File identification tools such as DROID can be used to scan entire file stores and identify not only files in this particular format, but more widely identify the formats your organisation is using and which ones may be unsupported or at risk. A high volume of business critical information in an obscure format is a risk – and may justify the cost/time of restoration (where restoration is possible).

Longer term you may also wish to:

- identify your business critical information – make sure your Information Asset Register is accurate and up to date
- put in place systems to ensure your IT and information management teams work more closely together, especially when you are planning system changes, to ensure that business needs for information use are built in at the outset.

Appendix: testing for continuity of a digital asset

This checklist helps test that your information asset meets your users' needs to find, open, work with, understand and trust the information it contains. The term 'user' refers to anyone with a business requirement to use the information. Remember that different users may have different needs: you will be unable to manage the digital continuity of your information asset unless you understand what these needs are. If you are not confident that your information asset and its supporting technology meet your users' requirements, you may have experienced a loss of digital continuity of the information asset.

1. **Can users find the information when they need it?**

□ Do users know where to look for the information?
Does it have a defined filing location?

□ Is the information where it should be?
Do users understand where to file it?
Do your systems make it easy to file in the right place?

□ Is the information searchable?
Is it indexed and covered by your search tools?
Do users have the correct permissions to enable them to find it?
Are the search tools easy to use?
Is it easy to identify information within the search results?

2. **Can users access and open the information when they need to?**

□ Can users retrieve the information when they need it?
Do they have the required privileges to access it?
Is it available to them within an acceptable timeframe?
Do they have the required hardware to access it?

□ Can users open or render files as required?
Do they have the necessary encryption keys or passwords?
Do they have the right software to open or view the file?
Is the file corrupt or otherwise un-openable?

3. **Can users work with the information as they need?**

□ Does the environment enable users to work with the information?
Do they have the required permissions to work with it?
Can they apply access controls to protect it as needed?

□ Do users have the right technology and tools to use it as needed?
Can users view, edit, share, publish or save it as needed?

□ Do data structures and file formats support using the information?
Can users manipulate, query, combine or report on it as needed?

□ Is the information complete?
Are all embedded objects, elements, links or relationships present?
Is any data corrupt or otherwise unusable?
Does data quality adequately support the task being undertaken?
Is the required supporting documentation available?

4. **Can users understand the information?**

□ Can users understand what the information is about?
Does its position in the filing structure tell the user what it is about?
Does its metadata describe what it is?
Is its scope or coverage clear?

□ Can users understand what the information is for?
Is it on an information asset list that states its business use?
Does its position in the filing structure indicate what it is used for?

□ Can users determine how the information was created and used?
Does its metadata describe why it was created?
Does its metadata describe how it is used?

5. **Can users trust the information?**

□ Can users trust the accuracy of the information?
Do they understand the assumptions made when it was created?
Do they trust the accuracy of each data element?

□ Can users trust the history of the information?
Do they know where the information came from?
Do they know how it has been handled and used?
Do they know who it has been shared with?

□ Can users trust that the information is authentic?
Is there reliable evidence of how and when it was accessed, changed, exported or copied and by whom?
Can they determine which version is current?