The National Archives

Digital Continuity to Support Forensic Readiness

This guidance is produced by the Digital Continuity Project and is available from www.nationalarchives.gov.uk/dc-guidance

© Crown copyright 2011

You may re-use this document (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, visit http://www.nationalarchives.gov.uk/doc/open-government-licence/open-government-licence.htm or write to the Information Policy Team, The National Archives, Kew, Richmond, Surrey, TW9 4DU; or email: psi@nationalarchives.gsi.gov.uk .

Any enquiries regarding the content of this document should be sent to digitalcontinuity@nationalarchives.gsi.gov.uk

Contents

1. Introduction

Digital continuity is the ability to use your information in the way that you need, for as long as you need. This means managing digital information effectively through periods of change so it remains complete, available and therefore usable as required. Managing digital continuity can help to provide your organisation with assurance that you are effectively managing information to meet your forensic readiness requirements.

Digital continuity and forensic readiness are mutually supportive. If you are working through the process of managing your digital continuity,[1] the details of your forensic readiness policy will form one of the business requirements, and the forensic evidence must be evaluated as part of your information asset identification. If on the other hand you are developing your forensic readiness policy, you must consider the risks of losing the digital continuity of your evidence assets and guard against these losses.

You will need to ensure that your information management and IT teams understand those needs, and manage your organisation's information assets and technical environment to provide the usability you need. If your forensic readiness needs change, you need to update your information management and IT teams so that they, in turn, can update their information asset and IT management processes.

1.1 What is the purpose of this guidance?

This guidance will:

- help you understand what digital continuity is
- explain how digital continuity supports forensic readiness
- explain how you can manage the digital continuity of your forensic assets.

Digital Continuity and Forensic Readiness is part of a suite of guidance[2] that The National Archives has delivered as part of a digital continuity service for government, in consultation with central government departments.

[1] See more on the four-stage process of managing digital continuity in our guidance nationalarchives.gov.uk/information-management/our-services/dc-step-by-step-guidance.htm

[2] For more information and guidance, visit nationalarchives.gov.uk/dc-guidance

This guidance assumes you are familiar with, or working through the CESG Good Practice Guide on Forensic Readiness[3] which explains in detail your responsibilities, best practices and a template for the forensic readiness policy itself.

1.2 Who is this guidance for?

This guidance is targeted at the person responsible for forensic readiness in an organisation, generally the Senior Information Risk Owner (SIRO) or a delegated representative.

[3] CESG, Good Practice Guide No. 18, (2009) *Forensic Readiness,* Issue No: 1.0

2. What is digital continuity?

Managing digital continuity means managing information over time and through change so that it remains complete, available and therefore usable. The digital continuity of your information is maintained when your technology and information management processes support your information assets in meeting your business requirements both now, and in the future. This is when:

- you know **what information you have,** what it is about and where it is
- you understand **how you want to use it**, now and in the future
- your **technology and information management process enables** you to use your information, and is agile enough to cope with your changing requirements.

Digital continuity is achieved when your technology supports the business use you need from your information assets.

2.1 What does digital continuity loss look like?

Digital continuity loss can manifest itself in five ways, leaving you unable to:

- **find** the information you need
- **open** the information you need
- **use** the information in the way you need (e.g. to export it or filter it)
- **understand** what your information is about
- **trust** your information is what it says it is.

Sometimes it is possible to recover your information once digital continuity is lost, but this may be expensive, time consuming or not possible at all.

2.2 The process of managing digital continuity

The SIRO is required to ensure all information risks are recognised and managed in an organisation, and this includes risks to digital continuity. However, SIROs will likely delegate the responsibility for driving forward action on digital continuity to a Senior Responsible Owner (SRO) who may, for instance, be the Head of Knowledge and Information

Management (KIM). The SRO will then work alongside other members of the organisation including the IT team and the Information Asset Owners (IAOs).

The key stages in managing your digital continuity are:

- Stage 1: Plan for action
- Stage 2: Define your digital continuity requirements
- Stage 3: Assess and manage risks to digital continuity
- Stage 4: Maintain digital continuity

3. Digital continuity and forensic readiness

> 'Forensic Readiness is the achievement of an appropriate level of capability by an organisation in order for it to be able to collect, preserve, protect and analyse Digital Evidence so that this evidence can be effectively used in any legal matters, in disciplinary matters, in an employment tribunal or in a court of law'
> CESG, Good Practice Guide No. 18, *Forensic Readiness*

Digital continuity is vital to forensic readiness because once you have identified what evidence you may be required to produce, you must consider how you are going to retrieve and make use of that information when you need it.

Managing digital continuity – and including the business need for forensic readiness in that management – will ensure that you retain the usability you need from your information. The CESG Good Practice Guide on Forensic Readiness (Good Practice Guide No. 18) describes twelve significant principles that organisations should observe as part of their adoption of forensic readiness. Principles 9 and 10 are heavily related to digital continuity:

Principle 9 – "Organisations should maintain the quality and effectiveness of their records management systems in order that specific business records can be produced as evidence in court or to address any legal or regulatory requirement."[4]

Principle 10 – "Organisations should provide appropriate records retrieval processes and mechanisms in order that any requirement to disclose information can be efficiently and securely dealt with. Such disclosures MUST be handled in accordance with all relevant legislation and regulations."[5]

GPG 18 also states "It is important that the retrieval process is effective, efficient and secure… The technology and methods used should support the selective release of information so that the appropriate information can be retrieved and isolated for release."[6]

If you have lost the digital continuity of your evidence, you will not be able to retrieve it effectively and efficiently.

[4] CESG, Good Practice Guide No. 18, (2009) *Forensic Readiness,* Issue No: 1.0, p 29

[5] CESG, Good Practice Guide No. 18, (2009), p 30

[6] CESG, Good Practice Guide No. 18, (2009), p 31

4. Managing the digital continuity of your evidence

Your organisation may already have policies and processes in place to manage digital continuity. The organisation's SIRO or Head of KIM should be able to provide more information and make sure that your requirements and assets are included in the policies and processes if they have not already done so.

If however your organisation has not already included your requirements for digital continuity in the policies and processes, you can do it yourself. You can apply the four-stage process of managing digital continuity, described below, to just your own section of information without having to take on the responsibility of creating processes for the whole organisation.

4.1 Plan for action

You need to consider the scope of your work and your priorities. One of the most important aspects of both forensic readiness and digital continuity is the time-value of digital assets. Digital continuity is all about ensuring information is available over time and through change, so you must understand how long you need to keep information for – and set appropriate retention schedules for particular types of digital evidence.

Depending on the type of evidence you are creating, it may be that you should not keep information for any lengthy period of time, so it is possible that losing digital continuity is only a very minor risk to your forensic readiness. For example, you should not keep personal information longer than is necessary for the purpose for which it was created.

Other information needs to be subject to a similar review process – log files, for example, can be very large and difficult to search and it may not be necessary to keep them for more than 12 months.

4.2 Define your digital continuity requirements

The steps below are covered in greater detail by two pieces of guidance – *Identifying Information Assets and Business Requirements*[7] which will help you identify information

[7] See *Identifying Information Assets and Business Requirements* nationalarchives.gov.uk/documents/information-management/identify-information-assets.pdf

assets and their requirements and help you assemble an Information Asset Register (IAR), and *Mapping the Technical Dependencies of Information Assets and their Business Requirements*[8] which is aimed at your IT team and will help them to provide the information you need on the technology mapping.

4.2.1 Identify your information assets

As part of putting together your forensic readiness policy, you will have identified the sorts of information and evidence you need to gather and how you may need to use them. These are your information assets.[9] You should then compile the information you have on these assets and their requirements into an IAR.

4.2.2 Define how you need to use your information

How you need to use your information covers everything from how you find it, through how you access it to what you do with it. You must also consider any surrounding or supporting information which is important. There are five questions you will need to answer and record in your IAR:

1. How will you **find** the information? (i.e. where is it?)
2. Who can **access** the information and how? (i.e. who owns the information, who is the key contact regarding this asset? How quickly do you need to be able to access it? How long do you need it to be accessible for?)
3. What do you need to be able to **do** with the information? (i.e. do you need to able to read it, print it, publish it, share it with others, interrogate or query it, use it to generate reports?)
4. What do you need to be able to **understand** about your information? (i.e. what level of context do you need – what metadata exists? Do you need related information assets in order to interpret it?)
5. Do you **trust** your information is what it claims to be? (i.e. what do you need from your information in order for it to be used as evidence for a forensic investigation?)

[8] See *Mapping the Technical Dependencies of Information Assets* nationalarchives.gov.uk/documents/information-management/mapping-technical-dependencies.pdf

[9] '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.' For more on information assets, see *Identifying Information Assets and Business Requirements* nationalarchives.gov.uk/documents/information-management/identify-information-assets.pdf

For each of these issues you must consider what the requirements are at the moment, and how they might change over time. This will encompass the retention schedules imposed on your assets.

For forensic records, the security and access regimes are also very important and so should be covered in detail here.

These questions above form the core of digital continuity – what usability you need to maintain for your information over time and through change. 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.

4.2.3 Map the technical dependencies of your information assets

The next step is to put together a comprehensive list of the technologies that are required to support each of the information assets; this will help provide better understanding of where issues could arise day-to-day and through change. This audit will cover all aspects of technology that might impact upon your evidence – storage, backups, security, software, search tools. To do this we recommend liaising with your Head of IT who will be able to provide this information.

When you have gathered this information and added it against each record in your IAR, you will have a list of all your sources of evidence, their key information, how you need to use them, and the technology that they rely on. This list will allow you to manage your digital continuity in the future.

4.3 Assess and manage risks to digital continuity

The third stage of managing your digital continuity is to do an assessment to determine whether your assets are at risk of losing their digital continuity. For the purposes of forensic readiness, you will probably have noticed potential risks as you went through the process of identifying the assets and their requirements.

Key risks are not being able to find the information you are looking for and not being able to verify that it is what it claims to be. This risk assessment should be performed alongside the preparation of the rest of your forensic readiness policy which will cover the security issues.

Many of the risks to the sort of information assets you will be using for forensic readiness are technology related, so it is vital to work closely with your IT teams to perform risk assessments and take mitigating action. The risks should be documented and a follow up schedule planned.

You should assess your risks corresponding to the requirements you've outlined in section 4.4.2 above.

Key questions to ask yourself on the risks to your digital continuity requirements:

- Am I at risk of not being able to **find** the right information when I need to? Do I know where it's kept, how to find or search for it? What is the back up process, how is it being managed and how do I retrieve it?
- Am I at risk of not being able to **access** the information when I need it? What technology do I need to maintain in order to access it? What access permissions are needed?
- Am I going to be able to **use** the information as I need to? What technology might I need to maintain in order to use it? Do I need to keep it in a particular format in order to use it as I need to?
- Am I at risk of not being able to **understand** the information? What contextual or related information am I dependent on to be able to interpret it correctly?
- Am I at risk of not being able to **trust** in the information? How will I be able to use it as evidence and prove its authenticity and reliability?

4.4 Maintain digital continuity

Once you have documented your information and what the usability requirements are to enable it to be used as evidence, you must make sure that its digital continuity is protected through time and change.

As the digital continuity guidance makes clear,[10] the main risks to digital information are organisational and technological change. Information is most likely to be lost when systems are replaced or organisations restructured. It is important to understand how changes might

[10] See The National Archives' digital continuity guidance nationalarchives.gov.uk/dc-guidance

impact on the usability of your forensic assets and to see whether the information assets, technology and usability requirements will still align following change. It must be clear whether assets which have a long-term forensic value can continue to be accessible.

> **Principle 6** – "Organisations should closely integrate Forensic Readiness plans with incident management and other related business planning activities.
>
> It is important that Forensic Readiness is not treated as an isolated discipline as this would lead to both inefficiencies and inevitable conflict. Consider a situation where a digital forensic investigation is launched only to find the ICT target of interest has been rebuilt to apply a software upgrade: the evidence would have been destroyed."[11]

The IAR you have developed should provide a clear guide to which pieces of information are linked to which pieces of technology. Maintaining good communications between the information asset owners and the corresponding owners of the technologies means any changes can be planned so that they do not compromise the value of the information.

For more information on how to take care of your information assets through change, there will be several pieces of guidance[12] available on The National Archives' website.

[11] CESG, Good Practice Guide No. 18, (2009), p 26

[12] For more information and guidance, visit nationalarchives.gov.uk/digitalcontinuity

5. Further reading

The following texts will help you to find out more about forensic readiness:

- CESG, Good Practice Guide No. 18, (2009) *Forensic Readiness,* Issue No: 1.0
  Provides good practice that can help to define and implement an approach to the development of Forensic Readiness Policy and associated planning and practice activities. The guidance provided is generic and includes information on how it can be applied to suit the requirements of individual organisations.

- Rowlingson, R. (2004) 'A Ten Step Process for Forensic Readiness'*, International Journal of Digital Evidence,* Volume 2, Issue 3
  This paper is intended for those with responsibility for, or potential involvement in, computer investigations... The aim of this document is to present the outline of a forensic readiness planning process that an organisation can adopt and adapt to its specific requirements.
  You can download the paper here:
  http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.65.6706&rep=rep1&type=pdf

You can also read more guidance on managing digital continuity online:
nationalarchives.gov.uk/information-management/our-services/dc-step-by-step-guidance.htm