Digital Preservation **Handbook**

Institutional Strategies

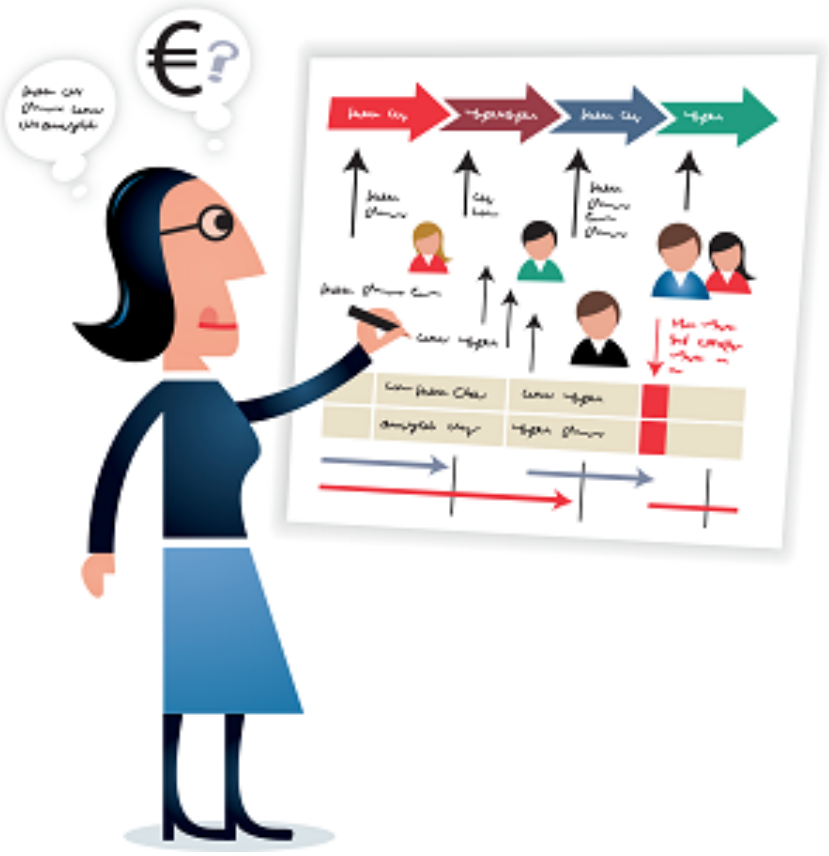


Illustration by Jørgen Stamp digitalbevaring.dk CC BY 2.5 Denmark

Who is it for?

Both senior administrators (DigCurV Executive Lens) and operational managers (DigCurV Manager Lens) within institutions. Also existing or potential third-party service providers.

Assumed Level of Knowledge

Intermediate (basic understanding of the issues, some practical experience).

Purpose

- To form the basis for further development of policies and strategies appropriate to individual institutions.
- To provide existing examples of good practice which might serve as models.
- This section outlines a number of strategies which have been used successfully by institutions in developing approaches to digital preservation. Each sub-section discusses the approach, its potential advantages and disadvantages, and then provides exemplars of the approach together with further reading on the topic. Strategies such as these will form a core component of corporate policy development to address digital preservation. Sound policy development combined with effective working practices and procedures (see Organisational activities) has been essential to effective digital preservation programmes.

Reusing this information

Contents

Institutional Policies and Strategies

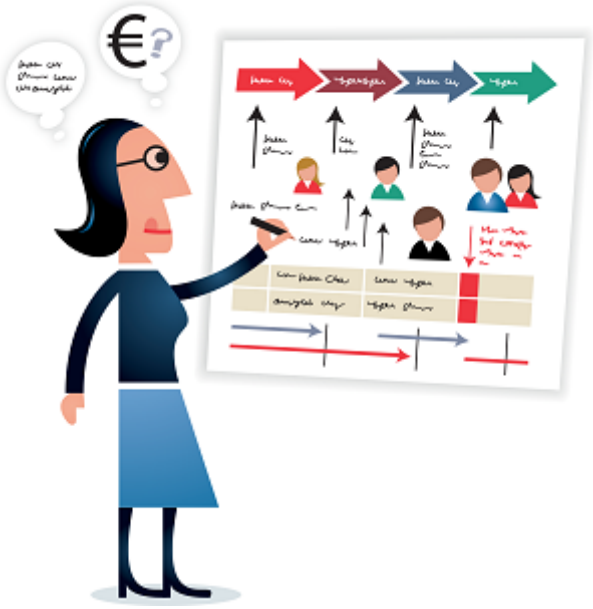


Illustration by Jørgen Stamp digitalbevaring.dk CC BY 2.5 Denmark

Introduction

The aim of this section is to help institutions understand, develop and implement digital preservation policies and strategies. These will help an organisation to set digital preservation goals, priorities and mechanisms that will also support the acquisition, life cycle management and dissemination of digital materials.

Policy and strategy are terms that are often used interchangeably or in different hierarchical sequence in different institutions. For consistency, the Handbook defines 'policy' as the highest level document and 'strategy' as the documents and procedures that support the implementation of the policy. In principle the development of policy precedes the development of strategy. In turn strategy may be developed or revised/reviewed on a regular basis, whereas policy may have a longer review cycle. Thus a policy serves the organisational need whilst individual strategies may serve different business units or divisions.

Policy and strategy documents provide a foundation upon which all activities around management of digital materials can be based. Policy and strategy documents that are well formed and consultative provide for high levels of both consensus and compliance in the day-to-day activities of managing digital materials. In turn, this provides for certainty that digital materials are being managed appropriately and to best effect. Policy documents also form the basis for cost planning and for funding applications. Strategy can be used as a flexible means to both adapt to changing situations and to demonstrate that learning that has been applied.

Within any institution there will be a range of stakeholders who have a stake in the life cycle management of digital materials. They may contribute to the management of those materials, they may create or manage metadata associated with those materials, or they may have management responsibility for collections. The end-users are also key stakeholders as their needs determine what is important for preservation. The views of stakeholders and their roles in relation to the management of digital materials must be considered at both the policy and strategy level.

You may find it useful to apply the iterative four-step management method of Plan–Do–Check – Adjust as a model for continuous improvement and effective development, implementation and revision of policies and strategies.

Digital preservation policy as part of the wider organisational context

If you are embarking upon, or thinking of embarking upon the creation of a digital preservation policy for your organisation, then it is necessary to start by investigating the context in which the policy will exist.

It is likely that a broad range of policy documents will already exist across your organisation covering a wide variety of issues such as staffing, information technology, risk assessment, and finance. There mayalso be a number of policies relating to more specific issues of records and collections management that will be relevant to digital preservation activities. It is essential to consider both the content and established style and structure of all relevant policies within the organisation as well as the how digital preservation policy will fit within the wider landscape. No single policy or strategy document can stand alone so to achieve support for and successful implementation of a digital preservation policy it is essential to embed it in the broader policy context.

Important considerations in developing policy and strategy

An important aspect of policy development is consideration of the specific needs of your organisation and its key drivers. Alignment with organisational business drivers ensures that strategy and its implementation are also aligned with business need. Policy and strategy documents should make explicit links with and between relevant and existing policies and strategies and build on existing practice. Collaboration, sharing and consultation with stakeholders are essential processes in the development of policy and strategy.

Digital preservation policies are ideally technology neutral, i.e. not dependent upon any one technology platform or system. However in reality this may be unachievable. In such cases they should be focused on principles, aims and objectives that the requisite technology can support.

In order to develop clear, coherent and robust documentation and processes it is essential to adhere to a set methodology and to establish a plan for review so that the policy and strategy remains relevant and current.

1. **Establish purpose**. The first step is to establish the main purpose of the digital preservation policy, its scope and key aims. These will keep the process of policy development focused and its content coherent. Thought should be given at this stage to how the document will used, both as a tool for advocacy and to help guide the creation and implementation of strategy.

2. **Research**. As expressed above, it is essential to understand the organisational context in which the policy will exist. Time should be spent investigating existing policy, understanding the organisation's business drivers and the needs of key stakeholder groups. This phase will also incorporate research into best practice for digital preservation policy and strategies, examining the tools and resources available as well as reading policies and strategies from other organisations. Many resources are available with suggestions of what to include in your digital preservation policy and strategy (see Resources).

3. I**dentify elements and develop structure**. Based on the research carried out in the previous phase, the main topics and issues to be addressed in the policy and strategy should be selected. Developing a clear structure for the documents is essential to ensure the

documents are useful in practice and to facilitate easy updates and review. The structure should reflect any standards or existing best practice for policy and strategy documents within the organisation.

4. **Develop content**. Policy content should be high-level and set broad aims and objectives. It should avoid identifying specifics such as details of particular technology solutions, although it may contain reference to commitments established on an organisational level. Information on practical application of the policy will be defined by relevant strategy documents. Content may also be aspirational in relation to aims and objectives but care must be taken not to set unobtainable goals. Recommendations on how to address specific issues within your policy and strategy are available from numerous sources (see Resources).

5. **Stakeholder review**. It is essential to gain buy-in from various stakeholder groups to ensure your policy and strategy are both fit for purpose and will have support from across the organisation. Presentation of the draft documents to key stakeholder groups is an important part of the drafting process and any feedback provided should be considered carefully. This can also be a key step in advocacy for digital preservation within your organisation, allowing stakeholders to feel engaged with the process and to understand how digital preservation activities relate to their own work. (see Advocacy)

6. **Gain approval**. Most organisations will require that new policy documents are officially ratified by your management board. Make sure to be aware of the process the organisation and any requirements that will need to be fulfilled. Once ratified the policy will carry more weight and as a result will be easier to implement as part of ongoing strategy.

7. **Regular reviews**. Policy and strategy documents should not be static and must be responsive to changes in stakeholder needs, the wider organisational context and updates to best practice. A regular review cycle should be established but may also be triggered by significant changes in any of the areas mentioned above.

8. **Implementation**. Establish an implementation plan to make policy and strategy a reality in terms of day-to-day operations. Remember they are a mean to an end, not an end in itself.

Resources

Digital Preservation Policies Study

http://www.webarchive.org.uk/wayback/archive/20140615022334/http://www.jisc.ac.uk/media/documents/programmes/preservation/jiscpolicy_p1finalreport.pdf

This JISC funded study published in 2008 created a model framework for a digital preservation policy and accompanying implementation clauses based on examination of existing digital preservation policies. Although focussing on the UK Higher and Further Education sectors, the study draws widely on policy and implementations from other sectors and countries.

An additional output was a series of mappings of digital preservation links to other key institutional strategies in UK universities and colleges with the aim of helping institutions and their staff to

develop appropriate digital preservation policies and clauses set in the context of broader institutional strategies. (60 pages).

Digital Preservation Policies: Guidance for archives

http://www.nationalarchives.gov.uk/documents/information-management/digital-preservation-policies-guidance-draft-v4.2.pdf

This guide published by The National Archives in 2011 explains the key characteristics of a digital preservation policy. It discusses why there is a need for a policy and how it supports digital preservation. The primary audience for the guidance is publicly funded archives. (16 pages).

Analysis of Current Digital Preservation Policies: Archives, Libraries and Museums

http://www.digitalpreservation.gov/documents/Analysis%20of%20Current%20Digital%20Preservation%20Policies.pdf?loclr=blogsig

This report published in 2013 by Madeline Sheldon, a Junior Fellow with NDIIPP at the Library of Congress, discusses the current state of digital preservation policy planning within cultural heritage organizations. The collection of new or recently revised digital preservation policies or strategies, published during 2008 and 2013, resulted in a high-level analysis of the contents within those documents. A summary overview of the findings was also made available as a post on The Signal blog. (23 pages).

APARSEN D35.1 Exemplar good governance structures and data policies

http://www.alliancepermanentaccess.org/index.php/consultancy/member-resources/documents-and-downloads/?did=174

This report summarises the level of preparedness for interoperable governance and data policies. It concludes with selected recommendations that should be taken into account when drawing up data policies concerning digital preservation. (2014, 43 pages).

SCAPE Catalogue of Preservation Policy Elements

http://wiki.opf-labs.org/display/SP/Catalogue+of+Preservation+Policy+Elements

The European Project SCAPE (2011 - 2014) was tasked with looking at policy and producing a catalogue of policy elements to assist those writing policy. This wiki gives some information on the background to the policy work and then has pages for each element which the SCAPE project suggested that organisations should consider when writing policy, with a focus of planning and watch activities. There is also the final report of this work made publicly available in February 2014 on the SCAPE website.

Published Preservation Policies

http://wiki.opf-labs.org/display/SP/Published+Preservation+Policies

An extensive web directory prepared by the SCAPE project in 2015 listing digital preservation policies that are publicly available online for libraries, archives, data centers, and miscellaneous institutions.

Case studies

A Digital Preservation Policy for Parliament

http://www.parliament.uk/documents/upload/digitalpreservationpolicy1.0.pdf

The purpose of this Policy published in 2009 is to state and communicate the principles that guide the UK Parliament's activities to secure the preservation of its digital information resources. Further policy documents, procedures, standards, and guidance will be developed in future to address specific aspects of the Strategy. (17 pages).

Hampshire Archives and Local Studies (HALS) Digital Preservation Policy

http://www3.hants.gov.uk/archives/hro-policies/hro-digital-preservation-policy.htm

To address the risk of losing digital materials, HALS has developed a digital preservation policy and strategy. The policy outlines the Record Office's approach to digital preservation, whilst the aim of the strategy is to describe this approach in more detail, including technical specifications where appropriate.

DPC case note: Cabinet papers - policy as a measure of commitment

http://www.dpconline.org/component/docman/doc_download/449-casenotecabinetpapers.pdf

This case note from The National Archives examines the relationship between policy and practice in digital preservation. Grant giving organisations should request copies of applicant's digital preservation policies when funding data creation, as these are an indication of the organisation's commitment to long-term access. The National Archives has digitised a significant volume of the UK's Cabinet Papers, and have a carefully considered policy framework for the long term management of digital resources. May 2010 (3 pages).

DPC case note: Welsh journals online: effective leadership for a common goal

http://www.dpconline.org/component/docman/doc_download/450-casenotewelshjournals.pdf

This Jisc-funded case study examines a complex digitisation project at the National Library of Wales, an example of an organisation where there are many stakeholders and many different skills are required. Nominating a single senior member of staff as the lead officer for digital preservation and allowing them to work across different sections of the institution mitigated the risk of uncertainty around responsibility for preservation actions. June 2010 (3 pages).

British Library Digital preservation strategy 2013-2016

http://www.bl.uk/aboutus/stratpolprog/collectioncare/digitalpreservation/strategy/dpstrategy.html

The British Library's Strategy includes four priorities. Each priority is accompanied by a series of actions. These priorities are aligned with the Library's overall approach to Collection Care and its five principles of sustainable stewardship: to predict, protect, prioritise, preserve, and enable.

Strategic Priority 1: Ensure our digital repository can store and preserve our collections for the long term

Strategic Priority 2: Manage the risks and challenges associated with digital preservation throughout the digital collection content lifecycle
Strategic Priority 3: Embed digital sustainability as an organisational principle for digital library planning and development
Strategic Priority 4: Benefit from collaboration with other national and international institutions on digital preservation initiatives

Further details of each can be found in the full version of the strategy in a linked pdf document (16 pages).

Wellcome Library's Preservation Policy

http://wellcomelibrary.org/what-we-do/library-strategy-and-policy/preservation-policy/

The purpose of the Wellcome Library's Preservation Policy is to provide a comprehensive statement on the preservation and conservation of the Library's collections. It is intended to cover all material in all formats. The policy contains three parts that cover general statements, the management of physical materials and the management of digital materials.(25 pages).

UK Data Archive Preservation Policy

http://data-archive.ac.uk/media/54776/ukda062-dps-preservationpolicy.pdf

This policy published in 2014 outlines the principles which underpin the main activities of the UK Data Archive (the Archive) the active preservation of digital resources for use and re-use within its core user community. From a preservation point of view this policy generally conforms to the OAIS Reference Model, with additions and alterations which are specific to the materials held within the Archive. The Archive has a series of strict requirements for its digital preservation activities. These requirements are laid down in this policy, and the manner in which these requirements can best be achieved in relation to regulatory requirements, archival best practice, information security and available funds is also detailed below. Consequently, the Archive's preservation policy is based upon open and available file formats, data migration and media refreshment. (16 pages)

Digital Preservation Strategies for a Small Private College

http://files.archivists.org/pubs/CampusCaseStudies/CASE-16-MegMiner-Final.pdf

The POWRR Project (2011 – 2014) investigated, evaluated, and recommended scalable digital preservation solutions for libraries with smaller amounts of data and/or fewer resources. Well established "best practices" in digital preservation (DP) do little to address day-to-day realities in repositories that cannot dedicate funds or staff to DP workflows. Meg Miner, Illinois Weslyan University, discusses what can be done to ensure good stewardship for born digital and digitized institutional records before a complete preservation system is in place. 2015 (13 pages).

University of Edinburgh - Developing a Digital Preservation Policy

http://www.dpconline.org/component/docman/doc_download/1321-making-progress-hsbc-nov-2014-lee

A great presentation and case study by Kirsty Lee at the University of Edinburgh to the DPC Making Progress in Digital Preservation workshop in October 2014 explaining the methodology that she is using to build a digital preservation policy at Edinburgh. (14 pages)

Collaboration

Illustration by Jørgen Stamp digitalbevaring.dk CC BY 2.5 Denmark

Introduction

There are compelling reasons and, in some cases, political pressure, to engage in greater collaboration within and between organisations in order effectively to confront and overcome the challenges of digital preservation. The range of skills required to do this demands flexibility within organisational structures to facilitate working in multi-disciplinary teams. There is a significant overlap in the digital preservation issues being faced by all organisations and across all sectors so it makes sense to pool expertise and experience. Communication with key stakeholders, using terms and language understood by them (see Advocacy) will play a major part in building and maintaining collaborations.

Internal collaboration

The usual assumption is that collaboration is external. However, most libraries and archives will be managing a combination of paper-based and digital resources for the foreseeable future and will need to structure their organisation to manage the disparate needs of the two. The blurring of boundaries and the lifecycle changes which digital technology produces means that sections and departments which are structurally distinct, will now need to co-operate in order to integrate the preservation and management of digital materials with other materials.

Such co-operation and joined-up working may well prove impossible unless there are mechanisms put in place to facilitate it and there is clear executive buy-in and sponsorship to promote action. At the strategic level, a cross disciplinary committee or project team charged with developing and overseeing objectives is one means of ensuring that all relevant sections can be brought together. At the operational level, consideration will need to be given to defining what specific tasks are required and where those responsibilities logically lie. Setting up of working groups to investigate specific issues is one means of blending the range of skills required. Good communication and advocacy to other stakeholders will also be important (see Advocacy).

Whilst the need for a policy or strategy relating to digital preservation may be well established within the repository team, the driver for internal collaboration is typically in response to a specific challenge faced by an organisation.

Advantages

- Makes good use of available skills and expertise and makes the case that digital preservation is an institutional issue and not one owned exclusively by the repository.
- Promotes cross-team working by improving understanding of shared objectives and who needs to contribute.
- The sooner digital preservation becomes part of the daily work of an organisation and its employees, the better it is for their transition to and readiness for a more digital world.
- Recognises the diversity of skills required for the digital environment in general and digital preservation in particular.
- Is more likely to be focused and aligned with institutional objectives and priorities.
- Maintains a high profile for the work.

Disadvantages

- May be frustrating and time consuming in the short term.
- Communication may be difficult initially - for example there are some issues surrounding terminology with the term 'archives' meaning different things to archivists and IT colleagues
- Senior management may be unwilling to risk perceived lack of control.
- Staff may feel uncomfortable with new ways of working.
- Organisational structures may not be sufficiently flexible to facilitate effective collaboration between different sections.

External collaboration

There may be a number of drivers for external collaboration. There is the simple desire for lone specialists to work with other professional colleagues and seek external validation of their ideas or direction of travel. At the other end of the scale is the response to external funding opportunities, with funders now placing greater emphasis on collaboration. Some examples of types of external collaboration in the digital preservation sector are included below:

- **Collaboration around a specific problem to make progress easier and more affordable**. The Digital Preservation Coalition itself is an example of this in the UK. Members are encouraged to engage and collaborate on a number of different digital preservation related issues both at a high level and on specific topics. Another example is the Section for Archives and Technology of the Archives and Records Association, which brings together members of the professional body to look at specific aspects of the work and to share current practice.
- **Collaboration around a standard**. An example of this would be the call in 2015 to work together around the revision of the OAIS reference model. In an initiative coordinated by the DPC, practitioners working in the field were encouraged to engage and feed into a shared response. (See http://wiki.dpconline.org/index.php?title=OAIS_Community)
- **Collaboration around a specific piece of software or system**. An example of this would be the user groups that evolve around digital preservation software solutions, both commercial and open source. When exploring a piece of software for the first time there is huge value in being able to share experiences and learn from others.

- **Collaboration within a specific geographical area**. There are many examples of organisations collaborating based on their geographical proximity and the ease of working together that this offers. One example of this is the Digital Preservation Group within Archives & Records Council Wales (ARCW) (see Case studies).

Advantages

- Organisational commitment and authority.
- Formal agreements offer a clear allocation of responsibilities between partners.
- Enhanced understanding of complex issues.
- Greater practical benefit from pooled resources and expertise.
- Enhanced reputation through successful delivery of a project or being able to manage digital preservation.
- Improved prospects for future mutually beneficial collaboration.

Disadvantages

- Difficulty of establishing unambiguous agreements able to be accepted by all parties.
- Time taken to establish teams or a collaborative framework.
- Difficulties of communicating across different professional and organisational frameworks.
- Potential bureaucratic barriers.

External collaboration can work on an informal or a formal basis and colleagues across the sector have always shared experiences, with informal collaboration often forming part of an individual's continuing professional development. Larger more complex collaborations are more likely to have a formal partnership agreement that can be useful to define the scope and boundaries of the working relationship and attribute specific responsibilities.

Resources

Benefits from Research Data Management in Universities for Industry and Not-for-Profit Research Partners

http://opus.bath.ac.uk/32509/

Applies a stakeholder mapping using the KRDS Benefits Framework to examine the data management benefits associated with Faculty-Industry and Faculty-Not-for-Profit research collaborations with the University of Bath. It presents a summary list of benefits to different stakeholders that can arise from research data management and data preservation in these collaborations.

Aligning National Approaches to Digital Preservation Conference Proceedings 2012

http://educopia.org/publications/anadp

This publication contains a collection of peer-reviewed essays that were developed by conference panels and attendees. It aims to establish a set of starting points for building a greater alignment across digital preservation initiatives and highlights the need for strategic international collaborations to support the preservation of our collective cultural memory (342 pages).

North West Region Digital Preservation Group

https://nwrdpg.wordpress.com/

The North West Region Digital Preservation Group is an example of an informal geographical collaboration involving local authority, academic and specialist archivists. Outcomes include guidelines for depositors, a workbook for archivists and pilot studies on web archiving and email archives.

Case studies

DPC case note: Welsh journals online: effective leadership for a common goal

http://www.dpconline.org/component/docman/doc_download/450-casenotewelshjournals.pdf

This Jisc-funded case study examines a complex digitisation project at the National Library of Wales, an example of an organisation where there are many stakeholders and many different skills are required. Nominating a single senior member of staff as the lead officer for digital preservation and allowing them to work across different sections of the institution mitigated the risk of uncertainty around responsibility for preservation actions. June 2010 (3 pages).

DPC case note: Freeze Frame preservation partnerships

http://www.dpconline.org/component/docman/doc_download/434-casenotefreezeframe.pdf

This case note examines the relationship between the relatively short lived Freeze Frame project at the Scott Polar Research Institute and the institutional repository which offered to provide long term preservation services to ensure ongoing access at the end of the project. The study shows that small organisations don't necessarily need to establish a sophisticated preservation infrastructure when they embark on digitisation. Partnership can bring unexpected benefits to both parties, but needs to be thoughtfully managed and documented. April 2010 (4 pages).

Community Action via UK LOCKSS Alliance

http://www.slideshare.net/edinadocumentationofficer/ukla-dpc-final

Presentation given by Adam Rusbridge at the Digital Preservation Coalition on Getting Started in Digital Preservation, 28 February 2011. It discusses the role of the UK LOCKSS Alliance and collaboration in e-journal preservation.

Archives & Records Council Wales Digital Preservation Working Group

http://www.nationalarchives.gov.uk/documents/Cloud-Storage-casestudy_Wales_2015.pdf

This National Archives case study discusses the experience of a cross-sectoral working group of Welsh archives cooperating to test a range of systems and service deployments in a proof of concept for cloud archiving. It explains the organisational context, the varied nature of their digital preservation requirements and approaches, and their experience with selecting, deploying and testing digital preservation in the cloud. January 2015 (10 pages).

A collaborative infrastructure for permanent access to digital heritage in The Netherlands

http://www.ncdd.nl/wp-content/uploads/2016/03/Network_Digital_Heritage_Netherlands.pdf

In 2014 the Network Digital Heritage (NDE) was set up in 2014 by a group of national organizations in the Netherlands. The network presented a strategy for the development of a national, cross-domain infrastructure of digital heritage facilities. One of the programmes focusses on digital preservation (Sustainable digital heritage). The aim of this programme is to work on the cross-sector sharing, utilisation, and scaling up of facilities for sustainable preservation and access, while devoting attention to cost management and the division of duties. This programme is carried out by the NCDD, the National Coalition for Digital Preservation. (3 pages).

The SPRUCE project

http://wiki.opf-labs.org/display/SPR/Home

The Sustainable PReservation Using Community Engagement (SPRUCE) project (2011-2013) sought to inspire, guide, support and enable HE, FE and cultural institutions to address digital preservation gaps and to use the knowledge gathered from this activity to articulate a compelling business case for digital preservation. This multi-institutional collaboration brought archivists and technology experts together through mashup events and a hackathon. Two key outputs from the project were the Business Case Toolkit (http://wiki.dpconline.org/index.php?title=Digital_Preservation_Business_Case_Toolkit) and COPTR (Community Owned digital Preservation Tool Registry) (see http://coptr.digipres.org/Main_Page).

Filling the Digital Preservation Gap Case Study

http://digital-archiving.blogspot.co.uk/2015/12/research-data-spring-case-study-for.html

A collaboration between the Universities of Hull and York. The aim of the project was to address a perceived gap in existing research data management infrastructures around the active preservation of the data. Both Hull and York had existing digital repositories and sufficient storage provision but were lacking systems and workflows for addressing the active preservation of data.

Advocacy

Illustration by Jørgen Stamp digitalbevaring.dk CC BY 2.5 Denmark

Introduction

Digital preservation relies on a wide range of skills and services, so digital preservation managers need to coordinate a diverse set of skills, policies, tools and services from disparate sources. For some organisations digital preservation is entirely new and the relevant resources will need to be assembled for the first time. Even established programmes will face new challenges and therefore the range of tools and services required may constantly change. Hence the ability to communicate with other staff, departments, and organisations has emerged as a key skill for successful digital preservation managers.

Because technology and staff continue to change, communication and advocacy must be an ongoing rather than a one-off activity.

In the early days of digital preservation, communication and advocacy involved blunt statements about the social and economic impact of data loss and obsolescence. As solutions have emerged, so messages have become more subtle.

Advocacy has become increasingly about identifying stakeholders and helping them understand:

- how their choices make digital collections more or less resilient; and
- the benefits they will accrue from the active management of well-formed and accessible digital materials
- the necessity of investment – whether time, money or other resources – and the extent to which it is required to achieve these benefits.

In an institutional setting this means understanding all the agents involved in a digital object lifecycle, helping them to prioritise and support those actions that make and keep collections robust, and discouraging those actions which put collections at risk.

Stakeholder Analysis

Stakeholder analysis starts with gaining a clear understanding of the organisation's digital preservation aims before identifying internal and external stakeholders who can influence those

goals. Having identified them, it is then possible to develop a plan that will convey your aims and engage them in the digital preservation process. Approaching this with a clear methodology in mind will produce the best results and will tie in with a number of other digital preservation activities such as policy and strategy development (see Institutional policies and strategies), creating a business case (see Costs, benefits, impact and business cases) and identifying relevant standards and best practice (see Standards and best practice).

The following steps will help facilitate a thorough analysis of stakeholders:

1. **Identify what you hope to achieve** through your digital preservation activities. This may include lists of the principal collections involved and the main aims and objectives as well as potential benefits (see Business cases, benefits, costs, and impact) that will accrue. This will provide a clear reference and focus for advocacy and can later be tailored to the various audiences that are identified.

2. **Identify the groups and individuals** that can inhibit or enable digital preservation activities. These may be internal or external, and any one stakeholder can have multiple roles. For example, you may identify information technology staff as a key group which may then in turn include an IT Services Manager, Programmers and Support Staff. Some of these may be easily accessible inside your own department, some fall within different line management structures, and some will be entirely external. This means you may need to include other managers or service owners within your stakeholder analysis.

3. **Organise the stakeholder groups and individuals into key audiences** that are in a position to influence your goals and priorities. The audiences chosen will probably reflect the working practices of your organisation and/or your approach to digital preservation, perhaps relating to specific parts of your organisational structure (e.g. Senior Management, IT, Information Managers) or by their role in relation to the digital preservation process (e.g. Funders, Depositors, Users).

4. **Establish solid collaborative relationships with the key stakeholder audiences you have identified** to underpin progress towards the aims established in Step 1. Understanding the needs, priorities and constraints of internal and external stakeholders will yield information that directly informs your planning and improves your understanding of what stakeholders want and need from digital preservation activity. Stakeholders may be constrained by budget and/or legislative boundaries of which it will be valuable to be aware. Conversely, they may also have relevant expertise or resource that can be deployed towards digital preservation activity. In addition, understanding the language and terminology used by stakeholders enhances effective communication strategies and can help avoid difficulties that arise when stakeholders understand a term or concept in divergent ways. The ability to use your stakeholders' language generally helps get colleagues and collaborators to buy into your plans. If key stakeholders have conflicting interests you will need to mediate between them.

5. **Building on this two-way engagement, clearly define the important information to be shared with these audiences** that will help secure their buy-in. This should include:

    a Key messages based on your aims and objectives. These should be simple and direct statements written in plain language so they are easily understood by a wide range of

non-specialist audiences. Ideally they should also be aligned with wider organisational strategies and aims.

b Benefits that stakeholders will accrue from participation in/support of the proposed digital preservation activities. For example an IT manager might want to reduce costs of storage by deleting or de-duplicating redundant storage. A clear digital preservation strategy can help them reduce their storage requirements by distinguishing those collections that must be retained from those that are no longer required

c What will be required of them to ensure success. For example, you may wish to develop clear metadata requirements for depositors; or you may wish to give your IT department estimates for the amounts of storage and bandwidth that will be required and when.

d What barriers/misconceptions about digital preservation you may need to address. For example preservation is often confused with just having back-up copies. You may need to tailor language and terminology to specific audiences. For example certain terms such as "archiving" have different meanings in other sectors such as IT.

6. **Make a plan to engage each of the stakeholder groups** building on your knowledge of their priorities, expertise and limits, and using the various messages previously identified. You may need to use different methodologies for the various groups, tailoring your form of communication to best suit the audience and messages to be conveyed. This may include a range of communications channels including presentations, briefing papers and stakeholder working groups as well as developing a variety of plans and resources such as business cases (see Business cases, benefits, costs, and impact), policies (see Institutional policies and strategies) and risk registers (see Risk and change management).

Digital Preservation in the Media

Digital preservation gets surprisingly little attention in the mainstream media. Reporting of digital preservation tends to fall into two clichés: gloomy stories of data loss and an impending 'digital dark age'; or platitudinous statements about indestructible storage.

The reality is more mundane and more subtle. Practical, detailed and achievable requirements that deliver long term access, such as reported in this Handbook, are less attention-grabbing, but can deliver real benefits to institutions and their user communities.

In some advocacy contexts it may be useful to refer to a common vocabulary to support explanation of key terms and concepts in digital preservation. Some examples are suggested in the resources section below.

The broader digital preservation community has created short animations for advocacy such as those selected in the resources section below. These are short, entertaining, and often helpful in getting key messages about digital preservation across to non-specialist audiences and the general public.

Resources

Team Digital Preservation and Nuclear Disaster: An Animation

https://www.youtube.com/watch?v=pbBa6Oam7-w

Entertaining cartoon on the importance of trusted digital repositories, metadata, and refreshing digital media. (3 mins 18 secs)

Team Digital Preservation and the Aeroplane Disaster

https://www.youtube.com/watch?v=EKnsZZzuUr4

Entertaining cartoon on the effects of obsolescence and importance of migration. (3 mins 37 secs)

Team Digital Preservation and the Arctic Mountain Adventure

https://www.youtube.com/watch?v=PGFOZLecjTc

Entertaining cartoon on the importance of preservation planning. (4 mins 22 secs)

Team Digital Preservation and the Deadly Cryptic Conundrum

https://www.youtube.com/watch?v=Yun9hkPPF9M

Entertaining cartoon on the importance of representation information. (4 mins 9 secs)

Case Studies

Increasing Participation in Internal RDM Training Sessions

http://www.dcc.ac.uk/resources/developing-rdm-services/increasing-participation-training

This case study looks at the approaches taken by two Jisc MRD Projects to ensure good attendance at their internal research data management (RDM) training sessions. 2013 (4 pages).

Defining and Formalizing a Procedure for Archiving the Digital Version of the Schedule of Classes at the University of Michigan

http://files.archivists.org/pubs/CampusCaseStudies/Case2Final.pdf

Nancy Deromedi of the University of Michigan describes forming a partnership with a key administrative unit that had not been to date a receptive partner on campus, and raising the awareness of the archival considerations as the unit transitioned from a hybrid system of digital and paper to a solely digital process. April 2008 (8 pages).

Procurement and Third Party Services

Illustration by Jørgen Stamp digitalbevaring.dk CC BY 2.5 Denmark

Introduction

This section provides an overview of key issues and guidance in selecting and using and third-party services for digital preservation. The ways in which a service may be procured often vary according to sector or country. Individual organisations must identify and follow their statutory and regulatory purchasing policies to ensure that services are purchased using the correct procedures. Failure to purchase under the specific guidelines could lead to a serious issue possibly involving compensation to other potential contractors disadvantaged by incorrect purchasing processes.

Three tables are provided as part of the guidance: *Staff resources for procurement tasks*; *Issues and potential advantages and disadvantages of using third party services in digital preservation activities*; and a *Checklist for assessing storage readiness for digital preservation* as procurement is often a major component of implementing archival storage (see Storage and Cloud services). The final Resources section provides additional pointers to and summary description of further guidance and case studies.

Cost will clearly be a key consideration when deciding whether or not to contract out digital preservation but there are also other factors to consider and the advantages and disadvantages of each will need to be balanced against the overall mission of the institution. These include the contract, service level agreement, functionality and quality of the services provided, integration with the institution's processes and environment, disaster recovery and business continuity plans, ability to exit the service if needed, and how the service can be monitored and measured. For example, legal requirements for data privacy or confidentiality may influence whether outsourcing is appropriate or not given the jurisdiction of the service provider and where the service is physically located.

Outsourcing specific tasks or services is by no means a new phenomenon. Repositories have contracted out some of their operations for decades. This is an area in which lessons learned from outsourcing in other services can be of value. A major learning experience which is directly applicable to the digital environment is the critical importance of having sufficient staff resources and knowledge of the technology to be able to prepare effective specifications.

Staff resources for procurement tasks

The extent to which the potential advantages of using third party services can be maximised and the potential disadvantages minimised will be heavily dependent on dedicating staff resources to the following activities:

Staff resources for procurement tasks
Establishing the organizational remit and appropriate governance when selecting third-party services: • Advocate the digital preservation concept. • Involve the appropriate internal stakeholders early in your thinking. • Develop a communications strategy not just for your procurement team but for broader stakeholders. • Maintain an up to date risk register for the procurement. • Use the expertise within your organization: for example do you have a procurement section?
Establishing clear and realistic requirements: • Align business case with identified needs within organisation. This may take some time but is vital to achieving a good outcome. • Create an environment in which your stakeholders can contribute to the discourse and feel they have had input. • Learn from experience of others in digital preservation community as a whole: this could include reference site visits and/or sharing documentation and viewpoints. • Define which preservation functions are to be included, e.g. ingest; storage, preservation planning, curation and management activities. Are all activities to be outsourced to third party provider or just part of the digital preservation framework? • Distinguish between essential functionality and desirable 'added value' functionality: using a particular requirements methodology for example the MoSCoW template provides important discipline not just in the early procurement stages but for any project plan going forwards. • Have unambiguous and measurable requirements that you can use to clearly show the contractor if they are meeting them or underperforming.
Clarifying legal requirements: • Follow institutional and regulatory procurement requirements and processes. • Data Protection, FOI, other sensitive content and copyright will all need to be considered. • It is worth spending time upfront on negotiating your contracts and agreements with third party providers. Misunderstandings in the future are time consuming.

- If you require changes to the contract or agreement offered it is vital to secure them before signing any binding contract in law. Build in review points to the contract and understand what levers you have at your disposal.
- Ensure that you are not obligated to award a contract to provide you with flexibility up to that point.
- Ensure that you can terminate the contract in a minimally disruptive way if the contractor is not meeting the requirements of the contract. Where possible only pay for the goods and services you have received and not those that you may receive in the future.
- Clearly understand what services and products are being offered within the baseline costs of the contract and which will incur additional costs.
- Make all legal requirements, including the legal jurisdiction/governing law, available to potential contractors as early as possible in the procurement as this may greatly affect if they take part in the process.

Maintaining good communication between the contractor and the institution:

- Service Level Agreement to identify roles and responsibilities of each party.
- Access to technological infrastructure only or external staff time / development support also?
- The softer vendor relationship building skills are also important in this context.
- Is there an active user community for your chosen system that provides feedback and good interaction with the contractor?

Undertaking quality assurance checks:

- Establish responsibility for functions such as integrity checking.
- Match quality assurance checks with the measurable requirements you specified in the contract and ensure the supplier is meeting requirements or changing /correcting their practices to meet them.
- Audit / compliance with legal responsibilities.

Developing and monitoring the contract:

- This may seem premature but an exit strategy should be identified upfront. Digital preservation function will outlast commercial service provider and current technological infrastructure.
- Understand your rights regarding your data. Are there costs of retrieving data required for access or transfer to another provider?
- Be mindful of the market and financial models used by vendors. You may need to think outside the box as these models might not match the financial model prevalent in your organisation (capital expenditure vs revenue expenditure is one frequent dilemma).

- Awareness of any changes to technological environment for third party provider.
- Keep up to date with the market after you have concluded your procurement. You need to know how commercially robust your vendor is. Update your due diligence checking periodically.

These costs will need to be added to the overall contract costs when calculating the cost benefit of using third party services for digital preservation, bearing in mind that most of these costs will be or should be incurred even if preservation is not outsourced.

Issues and potential advantages and disadvantages of using third party services in digital preservation activities

Issue	Potential advantage of using 3rd party services	Potential disadvantage of using 3rd party services
Limited staff, skills and experience	• Provides specialist skills and experience which may not be available within the institution.	• Without some practical experience and expertise, it will be difficult to develop and monitor effective contracts. Without practical experience it will also be difficult to understand and communicate effectively the requirements of the organisation (or to assess whether they are technically feasible or not). • Without practical experience it will also be difficult to understand and communicate effectively the requirements of the organisation (or to assess whether they are technically feasible or not)
Costs	• Avoids the need to develop costly infrastructure (particularly important for small institutions). • If there are economies of scale, outsourcing may well be cost effective.	• There is very little established bench marking. It is still too new an area. • Risk of business failure. • Until the market increases there may be an over-dependence on one contractor.
Speed of deployment	• Allows action to be taken in the short to medium term, pending	• Unless there are adequate exit strategies, may be locked into an

	development of infrastructure.	outsourcing contract longer than intended.
Core competencies	• Allows the institution to focus on other aspects of service provision.	• Danger of either not developing or losing specialist skills base. Still need ability to make informed decisions.
Access considerations	• Monitoring usage may be more efficient (assuming the contractor has a demonstrated ability to deliver meaningful usage statistics). • There may be synergies and cost savings in outsourcing access and preservation together.	• • Difficult to control response times which may be unacceptably low and/or more costly, especially for high-use items. • May be difficult to forecast future needs in this area.
Rights Management	• Avoids what is often a resource intensive activity for the institution.	• May significantly increase the cost of the contract and/or complicate negotiations with third party rights holders.
Security	• Contract can guarantee security arrangements required by the institution.	• Lack of control, especially for sensitive material.
Quality control	• A watertight contract will build in stringent quality control requirements.	• Risk of loss or distortion may still be unacceptably high for highly significant and/or sensitive material.
Storage	• Access to professionally managed and experienced storage arrangements with easy replication of content and integrity checking.	• Issues of trust and legal considerations when storing sensitive data. • Difficult to anticipate the actual costs of some services e.g. cloud storage and computing because the organisation often does not know exactly how much service it will need. This is uncertainty can be reduced with experience.

Checklists for selecting and comparing service providers

Checklists and standards can be valuable starting points when considering or evaluating the use of third-party services as they are ready made lists that you can easily adopt or adapt to fit your needs. In particular, checklists help you identify things that you might otherwise forget to consider as well as helping you to express issues and requirements clearly.

Checklists work well when coupled to a maturity model. For example, the NDSA preservation levels allow a checklist to be constructed to see how well a service provider delivers to each level. An organisation identifies what level of maturity they need both now and in the future and then looks for service providers with matching levels.

Checklists and standards for repository services are valuable starting points because you can pick and choose the parts of the checklist that would apply to the specific services you seek. Examples of relevant checklists and standards are available in Resources and are also discussed in more detail in the Audit and certification section of the Handbook.

A Handbook checklist for assessing storage readiness for digital preservation is provided below:

Checklist: questions for your preservation storage service provider
☐ What level of redundancy does the storage system provide? How many physical locations is digital material held in? What is the geographical distance between them?
☐ Are different types of storage technology employed to mitigate/spread risk? For example online and off-line storage.
☐ If a file has become corrupted or unintentionally altered, how does this get detected and when does detection happen? Are audit trails or other forms of logging available to show that data integrity checks have been done and to show the result?
☐ What is the disaster recovery strategy, for example if a storage system fails or there is a natural disaster at a storage site then how are digital materials recovered? When was the last time this DR strategy was tested?
☐ What is the storage migration strategy to address technical obsolescence? What happens when the system is at the end of its life and content needs to be migrated to a new system? Is the content still accessible during this process?
☐ What is the exit strategy when using a given type of storage (e.g. onsite, cloud) for example what happens if the vendor of the storage system goes out of business?

- [ ] What measures are in place to contain corrupted or altered files, for example quarantining files to prevent them from being replicated?

- [ ] What security and auditing measures are in place to prevent unwanted access and/or modification of the digital materials?

- [ ] Who is responsible for monitoring and managing the storage system to ensure it is functioning correctly? Is there continuity of staff in cases of holiday, sickness or departures?

- [ ] What contracts, warranties or guarantees come with the storage solution or service that commit the vendor or supplier to support, recovery or replacement if there are any problems?

- [ ] What approach or support is in place for storage technology watch and risk assessment so that migrations, refreshes, upgrades or maintenance can be planned and executed in a timely way?

- [ ] Are the costs and risks clear so that a trade-off can be assessed and made between number of copies, type of storage, ease of access, and safety of the digital materials?

- [ ] What standards does the provider aim to comply with? (e.g. OAIS, Information Security Standards) Does it aim to achieve recognition as a trusted digital repository?

- [ ] How can the provider demonstrate they are doing what you have agreed?

Resources

OAIS: Open Archival Information Systems: Reference Model for an Open Archival Information System. Recommended practice

http://public.ccsds.org/publications/archive/650x0m2.pdf

Provides a useful shared terminology and functional model when identifying requirements for procuring third party digital preservation services. (135 pages).

Data Seal of Approval (DSA)

http://datasealofapproval.org/en/information/guidelines/

The Data Seal of Approval is a self-assessment process for digital archives, aimed specifically at those archives that hold data. This repository assessment includes a 16 point checklist.

ISO16363: 2012 Audit and certification of trustworthy digital repositories

http://www.iso16363.org/

ISO 16363 is an evidence-based audit framework for digital preservation consisting of more than 80 criteria that can be used for self-audit or external audit. The criteria used in the standard look across the entire organisation and not just the technical system in which collection content is stored. The CCSDS Magenta Book pre-print version of the standard is freely available at http://public.ccsds.org/publications/archive/652x0m1.pdf.

DIN 31644 Information and documentation - Criteria for trustworthy digital archives

http://files.dnb.de/nestor/materialien/nestor_mat_17_eng.pdf

The extended self-assessment process for digital archives is a helpful checklist developed by nestor on the basis of the DIN 31644 Information and documentation - Criteria for trustworthy digital archives standard.(44 pages).

The NDSA Levels of Digital Preservation: An Explanation and Uses

http://www.digitalpreservation.gov/ndsa/working_groups/documents/NDSA_Levels_Archiving_2013.pdf

The US National Digital Stewardship Alliance (NDSA) Preservation Levels are used widely throughout the Handbook and are helpful in thinking about many areas of digital preservation. There are also Mappings of NDSA preservation levels to cloud storage vendor profiles by AVPreserve.(7 pages).

Where to keep research data DCC Checklist for Evaluating Data Repositories

http://www.dcc.ac.uk/sites/default/files/documents/publications/Where%20to%20keep%20research%20data.pdf

A useful Digital Curation Centre checklist on where to keep research data safe that includes Service Level Agreement maturity levels. It is mainly concerned with external third-party repositories that offer a managed service to the UK research community.(20 pages).

The National Archives Cloud Storage Guidance

http://www.nationalarchives.gov.uk/archives-sector/digital-collections.htm

Provides information about procurement in the context of cloud computing services for preservation purposes, including case studies from several institutions (see below). It is particularly notable for its consideration of the legal issues.

DPC procuring preservation event

http://www.dpconline.org/events/previous-events/1150-procuring-preservation-writing-and-understanding-requirements-in-digital-preservation

For an overview of some of the elements of scoping requirements see the individual presentations listed. Presentations on Requirements analysis, and Procuring Preservation: hoops, hurdles and processes are particularly relevant.

Case studies

Archives & Records Council Wales Digital Preservation Working Group

http://www.nationalarchives.gov.uk/documents/Cloud-Storage-casestudy_Wales_2015.pdf

This case study discusses the experience of a cross-sectoral working group of Welsh archives cooperating to test a range of systems and service deployments in a proof of concept for cloud archiving. It explains the organisational context, the varied nature of their digital preservation requirements and approaches, and their experience with selecting, deploying and testing digital preservation in the cloud. The case study examined the open source Archivematica software with Microsoft's Windows Azure; Archivematica with CloudSigma; Preservica Cloud Edition and has begun testing Archivematica with Arkivum 100. January 2015 (10 pages).

Tate Gallery

http://www.nationalarchives.gov.uk/documents/Cloud-Storage-casestudy_Tate_Gallery_2015.pdf

This case study discusses the experience of developing a shared digital archive for the Tate's four physical locations powered by a commercial storage system from Arkivum. It explains the organisational context, the nature of their digital preservation requirements and approaches, and their rationale for selecting Arkivum's on-premise solution, "Arkivum/OnSite" in preference to any cloud-based offerings. It concludes with the key lessons learned, and discusses plans for future development. January 2015 (7 pages).

Dorset History Centre

http://www.nationalarchives.gov.uk/documents/Cloud-Storage-case-study_Dorset_2015_%281%29.pdf

This case study covers the Dorset History Centre, a local government archive service. It explains the organisational context of the archive, the nature of its digital preservation requirements and approaches, its two year pilot project using Preservica Cloud Edition (a cloud-based digital preservation service), the archive's technical infrastructure, and the business case and funding for the pilot. It concludes with the key lessons they have learnt and future plans. January 2015 (9 pages).

Parliamentary Archives

http://www.nationalarchives.gov.uk/documents/Cloud-Storage-casestudy_Parliament_2015.pdf

This case study covers the Parliamentary Archives and their experience of procuring via the G-Cloud framework. For extra resilience/an exit strategy they have selected two cloud service providers with

different underlying storage infrastructures. This is an example of an archive using a hybrid set of storage solutions (part-public cloud and part-locally installed) for digital preservation as the archive has a locally installed preservation system (Preservica Enterprise Edition) which is integrated with cloud and local storage and is storing sensitive material locally, not in the cloud. January 2015 (6 pages).

Partnering with IT to Identify a Commercial Tool for Capturing Archival E-mail of University Executives at the University of Michigan

http://files.archivists.org/pubs/CampusCaseStudies/CASE-14-FINAL.pdf

Aprille Cooke McKay, Bentley Historical Library, University of Michigan, examines the challenges and opportunities of partnering with IT to issue a Request for Proposal (RFP) for commercial e-mail archiving software. 2013 (53 pages).

University of Sheffield Procurement Case Study

https://www.sheffield.ac.uk/library/special/speccoll

A summary of the process of procuring a digital preservation system at the University of Sheffield. (2 pages).

Audit and certification

Illustration by Jørgen Stamp digitalbevaring.dk CC BY 2.5 Denmark

Introduction

Organizations are increasingly interested in evaluating their digital preservation infrastructures against an assessment framework, and audit, certification, and self-assessment are hot topics in digital preservation. It is worth taking a moment to consider the difference between a self-assessment exercise and an audit.

Audit and certification is a formal process commonly carried out and delivered by external service providers. It is often a time consuming experience with exactingly high requirements that demonstrate to an external audience that a particular standard is being complied with.

Self-assessment is a precursor, or alternative, to a full audit and is typically delivered by staff inside of the organization, and the results are usually of highest value to the organization being assessed (rather than an external audience). Self-assessments can be useful in identifying practices which are underdeveloped and require improvement, particularly if an organization is interested in pursuing full audit and certification at a later date.

Many of the benefits can be summarised as ensuring that a repository can be trusted. The concept of a trusted or trustworthy digital repository is now broadly recognised in the digital preservation community. The following section summarises the work that has taken place over the past 10 - 15 years to get us to this point.

Background to development of audit and certification frameworks

Audit and certification methods for digital preservation implementations have been in development for well over a decade with different organizations developing different methodologies in parallel. In Europe these are now coalescing under the European Framework for Audit and Certification of Digital Repositories.

The OAIS Reference Model (ISO, 2012a) (see Standards and best practice) influenced the development of the different methodologies, which began with the publication of Trusted digital repositories: Attributes and responsibilities (RLG/OCLC, 2002). This was refined as the draft publication An audit checklist for the certification of trusted digital repositories (RLG-NARA, 2005) before being finalised as TRAC (Trustworthy Repositories Audit & Certification: Criteria and Checklist) (CRL, 2007).

Equivalent activity was also taking place in both the Netherlands and Germany. The self-assessment process, Data Seal of Approval developed by DANS (Data Archiving and Networked Services), was released in 2008. Meanwhile, based on recommendations from a working group of nestor, the German Standards Committee (DIN) adopted *DIN 31644 Information and documentation - Criteria for trustworthy digital archives*.

Following their publication of the OAIS standard, and the later adoption of OAIS as an ISO Standard, in September 2011 the Consultative Committee for Space Data Systems released recommended practice on "Audit and certification of trustworthy digital repositories", This was subsequently adopted and published as *ISO 16363 2012 Audit and certification of trustworthy digital repositories* (ISO,2012b).

Current assessment options and the European Framework for Audit and Certification

The apparent proliferation of repository audit standards has been frequently cited as a barrier to participation. Consequently the European Commission has hosted a series of meetings to discuss a European-wide approach, and there is now a Memorandum of Understanding to define a European Framework for Audit and Certification of Digital Repositories. This memorandum effectively creates a tiered approach to certification, allowing an entry-level self-assessment and peer review based on the Data Seal of Approval, a more extensive self- assessment (based on DIN 31644 or ISO 16363), and a full scale external audit based on ISO 16363.

1. Data Seal of Approval

The Data Seal of Approval (DSA, 2008) is a self-assessment process for digital archives, aimed specifically at those archives that hold data. Though an outlay of time is needed to apply for the DSA,

it is far less onerous than ISO 16363, having only sixteen guidelines on which the organisation is assessed. The guidelines are based on the following five criteria:

- The data can be found on the Internet;
- The data are accessible (clear rights and licences);
- The data are in a usable format;
- The data are reliable;
- The data are identified in a unique and persistent way so that they can be referred to.

Though the DSA is on the surface a self-audit, this self-audit is then peer reviewed before a seal is awarded, thus adding a level of authority to the process. Openness and transparency are encouraged and institutions are asked to make their evidence (essentially documentation, policies and procedures) freely available online. Unlike an audit under ISO 16363, the peer reviewer is not required to visit the institution to see that the policies and procedures are working in practice, so this process is very much based on trust.

DSA are in the final stages of reviewing proposed amendments to the DSA Guidelines as a result of work with the World Data System through the Research Data Alliance. Details of when and how the transition to new guidelines will be managed will be released in due course, but in the meantime the current seal will be extended through 2017.

2. DIN 31644 Information and documentation - Criteria for trustworthy digital archives

The DIN Standards Committee in Germany adopted *DIN 31644 Information and documentation - Criteria for trustworthy digital archives* based on recommendations from a working group of the German competence network for digital preservation (nestor). The standard consists of requirements for a trustworthy digital repository structured in three sections:

The **organisational framework** requires that:

- The repository has defined goals for the selection of digital material and accepts the responsibility to preserve them over the long- term;
- The repository has a defined community for whom access and the ability to interpret digital materials will be provided;
- There is observation of legal and contractual rules between data creators and the digital repository;
- Sufficient organizational structures are provided in terms of personnel, finance, long-term planning and continuity of service;
- Processes and responsibilities are defined and documented.

Object management requires that:

- The integrity and authenticity of digital material are maintained;
- A strategic plan for digital preservation activities is in place;
- Information packages for ingest, storage and dissemination are defined;

- Adequate documentation is provided including permanent identifiers and sufficient structural, technical, rights and change metadata;
- The digital material and related metadata are packaged together for permanent preservation.

Infrastructure and security requires that:

- The IT infrastructure can deal with the digital material adequately and is secure.

DIN 31644 is in German but an English translation is provided by nestor on their website.

The extended certification process undertaken by nestor takes about three months. Guidance on this process, (nestor Certification Working Group, 2013) is available on their website. This certification process should not be confused with full external audit- this requires formal accreditation under ISO 16363.

3. ISO 16363 Audit and certification of trustworthy digital repositories

ISO 16363 is an evidence-based audit framework that uses the term 'repository' to mean the organisation responsible for digital preservation rather than just the technical infrastructure being used for storage. The criteria used in the standard look across the entire organisation and not just the technical system in which collection content is stored. Metrics are grouped into three areas:

- **Organizational Infrastructure**: including governance, organizational structure, staffing, procedural accountability, policy framework, financial sustainability and contracts, licensing and liabilities;
- **Digital Object Management**: including acquisition and ingest, preservation planning, creation and preservation of Archival Information Packages (AIPs), and information and access management;
- **Infrastructure and Security Risk Management**: including technical infrastructure, risk management and security risk management.

Terminology used in ISO 16363 is directly aligned with that of OAIS and the standard asks directly about both OAIS information packages and functional areas. A basic understanding of OAIS is therefore useful for those seeking to understand ISO 16363 and deliver an assessment against it.

With over 100 metrics spread across the three areas, undertaking an ISO 16363 audit or assessment is a significant commitment similar to many other ISO standards applied across organisations. A relatively small number of organisations have utilised the ISO 16363 standard since it was published. Some have sought certification by external auditors whilst others have undertaken self-assessments. Houghton (2015) acknowledges that even though a self-assessment is not an audit it is nonetheless a significant undertaking that should be tailored to organisational circumstances.

ISO 16363 follows ISO practice for certification which assumes that those carrying out the audit are themselves certified. Two other ISO standards support this:

- *ISO 16919 Requirements for bodies providing audit and certification of candidate trustworthy digital repositories* (ISO, 2011) that sets out the requirements for any organisation that certifies the auditors for ISO 16363; and
- *ISO 17021 Requirements for bodies providing audit and certification of management systems* (ISO, 2012a) provides a mechanism to audit accreditation bodies.

An agency called PTAB (Primary Trustworthy Digital Repository Authorisation Body) offers training for auditors and those preparing for audit. Other agencies including the Center for Research Libraries are also providing audits against these standards.

4. Other frameworks and tools for self-assessment

A useful entry level resource is the Levels of Digital Preservation from NDSA (NDSA, 2013). This is particularly useful for those institutions that are just starting on starting out and can be used to benchmark initial steps. The NDSA levels are used extensively in the Handbook (see Getting started, Fixity and checksums, Information security, and Storage). Risk assessment frameworks and tools can also contribute to audit assessments (see Risk and change management).

Which audit or assessment option should I choose?

The 2010 Memorandum of Understanding described above, effectively identifies a tiered approach to certification. The amount of effort required for each level increases, though so does the formality of the output. The choice of assessment framework for any given organisation should therefore take at least the following into consideration:

Selecting an assessment framework	
What do you want to achieve from your audit?	What level of trust are you trying to engender? Do you seek certification from an external authority, or is self-assessment sufficient?
How much effort or funding is available to deliver the assessment?	ISO 16363 is a large undertaking that requires a significant amount of effort to gather the available evidence and run the audit; DSA has far fewer metrics and can be completed in a much shorter period. DIN 31644 has two assessment options with varying effort needed.
What type of content does your institution hold?	To date, DSA has been specifically developed for data-holding repositories, while DIN and ISO 16363 are both content-type neutral.
What framework, if any, will carry most weight in your organization or with your external stakeholders?	Is there any national preference for a framework or a framework commonly used by similar organisations that you should use?

The choice of assessment framework should not be made independently and can often be directly influenced by the value that an assessment may have for other parts of the organization. Discussing the options with organizational peers and managers can be a useful first step in ensuring the right option is selected and support is secured from other areas of the organization from the outset.

How to run an audit or self-assessment

Once an appropriate methodology has been selected, a straightforward way to proceed is to develop the initiative as a project and produce a project plan. Advice on project planning is prolific online and you should consult this if your organization does not have an agreed process for project management. If it does have a process, then you should become familiar with it and plan your project using this methodology (or secure the assistance of a local project manager). Your plan should include at least the following sections:

- Scope: What content is in scope of the assessment?
- Timeframe: When will the assessment take place and when will it deliver results?

- Stakeholders: Who will deliver the assessment? Who else needs to be interviewed or consulted?
- Governance: Which group will have governance of the assessment and results?
- Communications: How will the process and outcome be communicated to stakeholders?
- Next steps: How will the results be implemented?

If you are running an ISO 16363 assessment you should consult the advice on the ISO 16363 Primary Trustworthy Digital Repository Authority Body website. The audit preparation page outlines the steps that should be taken when running a full audit and these can be adapted for a self-assessment. Similarly, the Data Seal of Approval website has an online self-assessment tool that will guide you through an assessment. PDF or HTML versions of the assessment manual guidelines are also available.

Resources

APARSEN Report on Peer Review of Digital Repositories

http://www.alliancepermanentaccess.org/wp-content/uploads/downloads/2012/04/APARSEN-REP-D33_1B-01-1_0.pdf

Lessons learnt to date from the process of repository certification have been usefully summarized by the APARSEN project in this report. It suggests although there has been considerable progress, arguably audit procedures are not yet fully bedded down and some issues remain for both auditors and repositories. (2012, 50 pages).

Digital Preservation Management tools: Principles

http://dpworkshop.org/workshops/management-tools/principles

For organizations that are committed to becoming a Trusted Digital Repositories (TDR), a formative step for developing a sustainable digital preservation and curation program is to adapt and adopt a set of standards-based principles as a foundation. The principles provide a frame for your program and adopting them is a positive (and hopefully easy) place to start.

Digital Preservation Management tools: Model document

http://dpworkshop.org/workshops/management-tools/policy-framework

Every Trusted Digital Repository needs to have a high-level policy document that explicitly states the scope, purpose, objectives, operating principles, and context of the organization's digital curation and preservation program. The DPM workshop team developed this model document to help

organizations meet this objective. A model document identifies the recommended sections of a digital preservation policy framework with descriptions and examples for each section.

Digital Preservation Management tools: Self-assessment and peer review audit

http://dpworkshop.org/workshops/management-tools/self-assessment

TRAC (Trustworthy Repository Audit and Certification) Review tool developed for the DPM workshop.

The Open Archival Information System (OAIS) Reference Model: Introductory Guide (2nd Edition)

http://dx.doi.org/10.7207/twr14-02

This DPC Technology Watch Report from 2014 provides an accessible short guide to the OAIS standard. Terminology used in ISO 16363 is directly aligned with that of OAIS. The report will help provide a basic understanding of OAIS useful for understanding ISO 16363 and deliver an assessment against it.

Digital Preservation Capability Maturity Model (DPCMM)

https://lib.stanford.edu/files/pasig-jan2012/12F2%20Digital%20Preservation%20Capability%20Maturity%20Model%20in%20Action.pdf

This presentation describes a Digital Preservation Capability Maturity Model (DPCMM) that employs performance metrics based on specifications of ISO 14721 (ISO, 2012a),TRAC, and other good practices. (25 pages).

Data Seal of Approval

http://www.datasealofapproval.org/

In addition to the ISO standards developed by CCSDS, other formal initiatives in this area of archive certification have been the Data Seal of Approval (DSA), and the German Standard on Trustworthy Archive Certification DIN 31644.

European Framework for Audit and Certification of Digital Repositories

http://www.trusteddigitalrepository.eu/Site/Welcome.html

In 2010, the European Framework for Audit and Certification of Digital Repositories was established as a collaboration between the Data Seal of Approval (DSA) certification, the Repository Audit and Certification Working Group of the CCSDS, and the German Standards (DIN 31644) Working Group on Trustworthy Archives Certification. It aims to support an integrated framework for auditing and certifying digital repositories consisting of a sequence of three levels, in increasing trustworthiness.

Case Studies

Preserving the H-Net Academic Electronic Mail Lists

http://files.archivists.org/pubs/CampusCaseStudies/Case11Final.pdf

Lisa M. Schmidt, Michigan State University, describes assessing the existing state of preservation for the H-Net e-mail lists using digital preservation theory and the Trusted Repositories Audit & Certification: Criteria and Checklist (TRAC) evaluation tool. Making recommendations and overseeing the implementation of improvements to make H-Net a trusted digital repository. Ensuring authenticity is the primary preservation issue. 2009 (15 pages).

ADS and the Data Seal of Approval – case study for the DCC

http://www.dcc.ac.uk/resources/case-studies/ads-dsa

Archaeology Data Service colleagues Jenny Mitcham and Catherine Hardman describe the ADS experience in applying for the Data Seal of Approval (DSA). They identify practical information about the DSA application process. They also outline issues ADS faced in undertaking the process and the potential benefits they envisage from DSA self-certification. 2011.

Self-assessment of the Digital Repository at the State and University Library, Denmark – a Case Study

https://ipres-conference.org/ipres14/sites/default/files/upload/iPres-Proceedings-final.pdf

In this iPres 2014 paper, the authors describe the process and the benefits of performing an audit based on self-assessment and ISO 16363 for the digital repository of the State and University Library in Denmark. (p.272-279 of 385).

TRAC Audit: Lessons

http://blog.dshr.org/2014/08/trac-audit-lessons.html

This is the third in a series of blog posts by David Rosenthal about CRL's TRAC audit of the CLOCKSS Archive. Previous posts announced the release of the certification report, and recounted the audit process. This post look at the lessons CLOCKSS and others can learn from their experiences during the audit.

Trustworthiness: Self-assessment of an Institutional Repository against ISO 16363-2012

http://www.dlib.org/dlib/march15/houghton/03houghton.print.html

In 2013, Deakin University Library undertook a self-assessment against the ISO 16363 criteria. This experience culminated in the current report, which provides an appraisal of ISO 16363, the assessment process, and advice for others considering embarking on a similar venture.

Managing an ISO 16363 Self-Assessment: A How-To Guide

http://www.dcc.ac.uk/sites/default/files/documents/IDCC16/18_Managing_ISO16363.pdf

A short poster presented at the International Digital Curation Conference (IDCC) in 2016 by Maureen Pennock and Caylin Smith of the British Library.

References

CRL, 2007. *Trustworthy Repositories Audit & Certification: Criteria and Checklist*. Available: http://www.crl.edu/sites/default/files/d6/attachments/pages/trac_0.pdf

DIN, 2012, *DIN 31644 Information and documentation – Criteria for Trusted Digital Repositories*. Available: http://www.nabd.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738855&artid=147058907&languageid=de&bcrumblevel=3&subcommitteeid=112656173

Houghton, B., 2015. *Trustworthiness: Self-assessment of an institutional repository against ISO 16363-2012*. DLib Magazine, 21(3/4). Available: http://www.dlib.org/dlib/march15/houghton/03houghton.html

ISO, 2011. *ISO 16919:2011 - Space data and information transfer systems - Requirements for bodies providing audit and certification of candidate trustworthy digital repositories*. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=57950

ISO, 2012a. *ISO 14721:2012 - Space Data and Information Transfer Systems – Open Archival Information System (OAIS) – Reference Model*, 2nd edn. Geneva: International Organization for Standardization. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=57284

ISO, 2012b. *ISO 16363:2012 - Space data and information transfer systems – Audit and certification of trustworthy digital repositories*. Geneva: International Organization for Standardization. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56510

NDSA, 2013. *The NDSA Levels of Digital Preservation: An Explanation and Uses, version 1 2013*. National Digital Stewardship Alliance. Available: http://www.digitalpreservation.gov/ndsa/working_groups/documents/NDSA_Levels_Archiving_2013.pdf

nestor Certification Working Group, 2013. *Explanatory notes on the nestor Seal for Trustworthy Digital Archives*, nestor Materials 17, July 2013. Available: http://files.dnb.de/nestor/materialien/nestor_mat_17_eng.pdf

RLG/OCLC Working Group on Digital Archive Attributes, 2002. *Trusted digital repositories: Attributes and responsibilities*, Mountain View, California. Available: http://www.oclc.org/content/dam/research/activities/trustedrep/repositories.pdf

RLG-NARA Task Force on Digital Repository Certification, 2005. *An audit checklist for the certification of trusted digital repositories*, Mountain View. Available: https://web.archive.org/web/20051126181100/http://www.rlg.org/en/pdfs/rlgnara-repositorieschecklist.pdf

Legal compliance

Illustration by Jørgen Stamp digitalbevaring.dk CC BY 2.5 Denmark

Introduction

The information provided in this section is intended solely as general guidance on the legal issues arising from various aspects of digital archiving and preservation and is not legal advice. It does not attempt to provide guidance on general legal issues which impact on the operations of libraries, archives and other repositories, as these are covered in a number of other reference works. It is written from a UK perspective and legislation in this area will vary from country to country. Although it principally covers UK and European legal issues, many of the topics will also apply in general terms to other jurisdictions.

An adviser–client relationship is not created by the information provided. If you need more details pertaining to your rights and obligations, or legal advice about what action to take, please contact a legal adviser or solicitor.

Legal issues

'those engaged in digital preservation must work within the law as it stands. This requires both a good general knowledge of what the law is, and a degree of pragmatism in its application to preservation work. Such knowledge enables the archivist to avoid the pitfalls of over-cautiousness and undue risk aversion, and to more accurately assess the risks and benefits of taking on the preservation of new iterations of digital work.' (Charlesworth, 2012, p.3)

Intellectual property rights (IPR) and preservation

Intellectual Property Rights (IPR) are a section of UK law that include patents, trademarks, copyright and associated rights - such as the moral rights of the author (see Stakeholders, contract and grant conditions) and performance rights. The preservation of digital materials often requires the use of on a range of strategies, and this creates IPR issues that are arguably more complex and significant for digital materials than for analogue media. If not addressed these can impede or even prevent preservation activities.

What is different about copyright and digital materials?

Among the range of IPRs, copyright has a specific importance when considering digital preservation actions. UK copyright law was developed with analogue material in mind. Traditional analogue materials are relatively stable, and well established legal and organisational frameworks for preservation are in place. The legal framework for undertaking preservation work on digital material

is not as well developed and good preservation practices are not always recognised, or allowed for, by existing provisions in current legislation.

Copyright makes a distinction between ownership of the physical manifestation of a work, such as a book or work of art, and the separate right to reproduce it (the right to copy). Digital material by nature does not align to this distinction and can cause confusion when applied in the field. In the case of digital material, core repository practices such as providing access to users and routine preservation activities, often involve the deliberate or inadvertent creation of copies. Without appropriate rights clearance, licences or statutory exceptions these copies may constitute copyright infringements. Digital material therefore poses a different set of considerations for repositories holding this category of content. In addition, unlike physical material, digital material requires consideration of dependencies such as hardware and software which all have their own separate intellectual property considerations.

A second significant difference is the relatively short commercial and technological lifespan of digital material. The duration of IPR in digital materials extends beyond both commercial 'shelf life' and in almost every case the technology on which they depend. This forms a three-fold issue, in terms of procuring licenses to replicate content, licences for software to access content, and rights clearance of "abandoned" digital material, in addition to the added urgency of undertaking these actions.

Copyright exceptions

Although the Copyrights, Design and Patent Act (1988) limits possible preservation actions for digital material, exceptions for archives, libraries and museums have been introduced to address the unique requirements for preserving it. From a preservation perspective the most important provision (Intellectual Property Office, 2014) is the right to produce any number of copies required for the purpose of preserving digital material. Another important exception is the dedicated terminal exception, which enables a digital copy (i.e. one of the copies created under the preservation exception), to be made available on a dedicated terminal accessible to walk in users. These provisions only extend to items held permanently in the collection. The exceptions enables those institutions covered by the exemptions to hold copies of material in various file formats and thereby adhere to what is considered good preservation practice while staying within the law. Note that the copyright exception provisions do not overrule the moral rights of the author which must still be considered when undertaking preservation work.

The exemption to copy for preservation does not however take into account the dependent nature of digital material, and third party software dependencies can still form a barrier to preservation actions. This is particularly an issue observed in preservation strategies which rely heavily on retaining the wider technical environment of the digital objects in question. For example, emulation as a preservation strategy requires use of original operating systems and software external to the repository's permanent collection (see Preservation action). It is important to consider the additional costs and time of maintaining relationships with third party rights holders that follow from dependencies not covered in the exceptions.

Orphan works

For institutions looking to publish digital surrogates of analogue material, the Orphan Works Licensing Scheme run by the UK's Intellectual Property Office, as well as the EU Orphan Works Exception are likely to impact digitisation work and planning. The Licensing Scheme allows for both commercial and (in the case of heritage institutions) non-commercial digitisation of any type of material in which it has not been possible to trace the rights holders of the material following a 'diligent search'. The licence is a pay scheme limited to a seven year period and for use exclusively in

the UK. Repositories need to plan and budget for renewal of such licenses. The EU Orphan Works Exception, on the other hand, is restricted to text based and audio visual works only (and artistic works as long as they are embedded in the former), and museums, libraries, archives, educational establishments and public broadcasters. Here, the benefit is that the diligent searches are self certified and the preservation copy of the work, created under the preservation exception, can be placed on line for non commercial uses, for example, thus assisting greatly with digitisation activities.

Access and security

Some of the additional complexity in copyright issues relates to the fact that digital materials are also easily copied and re-distributed. Rights holders are therefore particularly concerned with controlling access and potential infringements of copyright. Digital Rights Management technologies (DRM) developed to address these concerns and provide copyright measures, such as copy protection software for files and intentional physical errors to CD/DVDs, can inhibit or prevent actions needed for preservation. DRM technologies are also in themselves subject to obsolescence. These concerns over access and infringement need to be understood by organisations preserving digital materials when negotiating deposit agreements with rights holders, and addressed by both parties in negotiating rights and procedures for preservation. Having clear deposit procedures in place can mitigate future access issues (See Negotiating rights).

Web archives and legal deposit

The legal status of web archives and processes of electronic legal deposit vary from country to country: some governments have passed legal deposit legislation but restrict access solely to library reading rooms. In others there is no legal deposit legislation and collections are either built solely on a selective and permissions basis or are held in 'dark archives' that are inaccessible to the public. In the UK, legal deposit libraries have the right to gather and provide access to copies of all websites published in the UK domain. However, access to the collection is restricted to library reading rooms (See Milligan, 2015). Parallel to this, Web Archives maintained by The National Archives (UK) operate with a smaller scope relating to government publications and clearer statutory powers derived from public records legislation (see Other statutory requirements).

The US-based Internet Archive, probably the largest and most used web archive, has no explicit legislative permission to harvest websites or to publish them. It operates on a 'silence is consent' approach, deleting from their collections any websites that an owner requests to be removed. In contrast, the Library of Congress operates on a permission basis meaning that they have to seek explicit approval from copyright holders before harvesting or publishing their content.

Other statutory requirements

Other statutory requirements may also apply and influence preservation of digital resources.

The requirements of public records legislation and the related expectations of the Freedom of Information Act apply to government records including those in digital form. Statutory and regulatory retention periods apply to many digital records (e.g. for accounting and tax purposes). Although these are often of limited duration, it is notable that requirements for retention of digital records in some sectors (e.g. the pharmaceutical industry, social care and health records), are of increasingly long duration. In such cases long-term preservation strategies will apply as technological change will almost certainly affect access to such records.

Information may be subject to data protection laws and relevant privacy legislation protecting information held on individuals. In the UK, the Information Commissioner's Office oversees adherence to data protection and privacy issues.

Information can also be subject to confidentiality agreements. Privacy and confidentiality concerns may impact on how digital materials can be managed within the repository or by third parties, and made accessible for use. Data protection law also impacts on data movement outside of Europe - an important consideration for organisations investing in server space abroad.

EU rulings on an individual's right to have their personal information removed from Internet search engines in certain circumstances has a significant impact on the practices of organizations working with digital content sourced from the web (Koops, 2011). The obligation to avoid doing harm to individuals when saving their data over long periods of time is reflected in the principle of the right to be forgotten, through the implementation of Article 12 of Direction 95/46/EC in the case law of multiple European nations.

Stakeholders, contract and grant conditions

Some digital materials are the result of substantial financial investment by public funds (e.g. research councils) and/or publishers, and intellectual investment by individual scholars and authors. Each of these stakeholders may have an interest in preservation; the organisation preserving these will need to acquire permissions from them to safeguard and maximise the financial investment or the intellectual and cultural value of the work for future generations. Such interests could be manifested through contract, licence, and grant conditions or through statutory provision such as "moral rights" for the authors.

Investment in deposited materials by the repository

Holders of the material over many decades will almost certainly need to invest resources to generate revised documentation and metadata and generate new forms of the material if access is to be maintained. Additional IPR issues in this new investment need to be anticipated and future re-use of such materials considered. Where a depositor or licensor retains the right to withdraw materials from the archive and significant investment could be anticipated in these materials over time by the holding institution, withdrawal fees to compensate for any investment may be built into deposit agreements (See Negotiating rights).

Rights management

As outlined in Legal issues, it is important that licensing issues, copyright and any other intellectual property rights in digital resources to be preserved, are clearly identified and access conditions agreed with the depositor and/or rights holders. If the legal ownership of these rights is unclear or excessively fragmented it may be impractical to preserve the materials and for users to access them. Rights management should therefore be addressed as part of collection development and accession procedures and be built in to institutional strategies for preservation. The degree of control or scope for negotiation that institutions will have over rights will vary but in most cases institutional strategies in this area will help guide operational procedures. It will also be a crucial component of any preservation metadata (see Metadata and documentation) and access arrangements (see Access).

Negotiating rights

As the volume of digital materials grows and the complexity of rights and number of rights holders in digital media continues to expand, ad hoc negotiation between preservation agencies and depositors and between rights holders themselves becomes more onerous and less efficient. This is

particularly problematic for any UK organisations or activities not covered by the new copyright exceptions.

Development of model letters for staff clearing rights, model deposit agreements, and model licences and clauses covering preservation related activities helps to streamline and simplify such negotiations. Institutions should seek assistance from a legal advisor in drafting such models and providing guidance for staff on implementation or permissible variations in negotiations with rights holders.

A number of institutions have developed models which can be adopted or adapted for specific institutions and requirements. The procedures outlined below are a synthesis of current good practice.

Recommended procedures

- Use legal guidance to frame your rights management policy and to develop documents.
- Develop model letters for rights clearance, model deposit agreements, model licences and clauses for preservation activities.
- If you are licensing material from third parties ensure they have addressed future access to subscribed material in the licence and have robust procedures to support this.
- Prepare reasoned arguments and explanations for your preservation activities suitable for external stakeholders such as rights holders who will need to be convinced of the need, and persuaded that their interests will be safeguarded. Remember their awareness of preservation issues may be low.
- Keep detailed records of rights negotiations. Make a schedule clearly identifying a list of materials deposited and covered by the licence. This will ensure that all that is believed to have been sent by the depositor has been received and may form the basis of an acknowledgement of receipt.
- Preserve information about rights and permissions for all your digital materials. Treat licences, schedules, and rights correspondence as key institutional records to be retained in fireproof and secure environments.

Summary of issues for licences and deposit agreements

The following provides a brief checklist and summary of legal issues which may need to be considered in relation to licences for preservation or deposit agreements for digital materials. Requirements will differ between institutions, sectors and countries and the list should be adapted to individual requirements. This list does not constitute legal advice and you must seek legal counsel for your specific circumstances.

IPR and digital preservation

A clause should be drafted to cover the following:

- Permissions needed for content.
- Permissions needed for associated software.
- Permissions needed for copying for the purposes of preservation. (A section which is applicable for material or organisations not covered by the copyright exceptions)

- Permissions needed for future migration of content to new formats for the purposes of preservation. (A section which is applicable for material or organisations not covered by the copyright exceptions)
- Permissions needed for emulation for the purposes of preservation.
- Permissions in respect of copyright protection mechanisms.

Access

- Permissions and conditions in respect of access to the material.

Statutory and contractual issues

- Statutory permissions and legal deposit obligations in respect of digital materials.
- Grant and contractual obligations in respect of digital materials.
- Conditions, rights and appropriate interests of authors, publishers and other funders.
- Confidential information and protection of the confidentiality of individuals and institutions.
- Protecting the integrity and reputation of data creators or other stakeholders.

Investment by the preservation agency

- IPR in any value added by the preservation agency.
- Withdrawal clauses (and associated fees).

Resources

UK legislation is regularly amended. To ensure that you are accessing the latest updates please refer directly to: http://www.legislation.gov.uk/

Exceptions to Copyright: Libraries, Archives and Museums

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/375956/Libraries_Archives_and_Museums.pdf

This guidance leaflet published by the Intellectual Property Office in 2014 sets out the exceptions applicable to libraries, archives and museums. It is relevant to anyone who works in or with libraries,

archives or museums in the UK, or copyright owners whose content is held by such institutions. In covers two significant changes in UK law which affect libraries, archives and museums. The first relates to making copies of works to preserve them for future generations. The second allows greater freedom to copy works for those carrying out non-commercial research and private study.

Intellectual Property Rights for Digital Preservation

http://dx.doi.org/10.7207/twr12-02

This DPC technology watch report was published by Andrew Charlesworth in 2012. The document does not cover recent legislation (such as The Legal Deposit Libraries (Non-Print Works) Regulations 2013 and the 2014 Copyright Exceptions for Libraries, Archives and Museums), but is otherwise a relevant introductory work. The report is aimed primarily at depositors, archivists and researchers/re-users of digital works. Intellectual property law, represented principally by copyright and its related rights, has been by far the most dominant, and often intractable, legal influence on digital preservation. It is essential for those engaging in digital preservation to be able to identify and implement practical and pragmatic strategies for handling legal risks relating to intellectual property rights in the pursuit of preservation and access objectives. (54 pages).

Aligning National Approaches to Digital Preservation

https://educopia.org/sites/educopia.org/files/publications/Aligning_National_Approaches_to_Digital_Preservation.pdf

These 2012 Proceedings include two papers on legal issues: Legal Alignment by Adrienne Muir, Dwayne Buttler, and Wilma Mossink (pgs 43-74); and Legal Deposit and Web Archiving by Adrienne Muir (pgs 75-88). The focus of the first paper is on the key issues of legal deposit, copyright exceptions for preservation and access, and multi-partner and cross-border working and rights management; the second paper discusses the challenges of adapting legal deposit a mechanism designed for print publishing to the digital environment. National approaches to key elements of legal deposit framework and the legal issues arising from non-statutory approaches to collecting digital publications for long-term preservation are identified.(342 pages).

Cloud Storage Guidance Appendix Table 3 - Legal Issues

http://www.nationalarchives.gov.uk/documents/CloudStorage-Guidance_March-2015.pdf

Table 3 provided in section 7 as an appendix to the TNA Cloud Storage Guidance published in 2015, lists legal points in greater detail for each of the three key categories:

- Any legal requirements in terms of management, preservation, and access placed upon archives and their parent organisations, by their donors and funders via contracts and agreements or via legislation by Government (e.g. accessibility, availability, information security, retention, audit and compliance, Public Records Act, etc.);
- Those legal obligations relating to third party rights in, or over, the data to be stored (e.g. copyright, data protection); and
- The legal elements of the relationship between an archive and a cloud service provider or providers (e.g. terms of service contracts and service level agreements).

Archives and Copyright: Risk and Reform, CREATe Working Paper No.3

http://www.create.ac.uk/wp-content/uploads/2013/04/CREATe-Working-Paper-No-3-v1-1.pdf

pages 6-18 of this 58 page 2013 paper by R. Deazley and V. Stobo, cover Copyright and the Archive sector within the UK.

A Layman's Guide to the KEEP Legal Studies

http://www.keepproject.eu/ezpub2/index.php?/eng/content/download/20703/103715/file/D2.6_laymansguidelegalstudies_final.pdf

This 2011 paper by D. Anderson of the KEEP (Keeping Emulation Environments Portable) Project (University of Portsmouth, National Library of the Netherlands) discusses the complicated and often contradictory legislative landscape for digital preservation activity in the European Union. Different nation states have their own. Over and above national law, there is the European Community framework, which is not uniformly or completely implemented across the whole of the EU. There is also non-EU legislation, and international treaties and obligations such as the Paris Convention for the Protection of Industrial Property (1883), and the Berne Convention for the Protection of Literary and Artistic Works (1886). The KEEP legal studies threw up two important issues: making copies of digital materials, and making these copies available to users. (39 pages).

Legalities Life Cycle Management

http://timbusproject.net/portal/domain-tools/72-portal/domain-tools/334-lehalities-lifecycle-management-tool

A tool developed by the TIMBUS project which looks at digital preservation of business processes. The areas covered are IPR, IT contracting, Data Protection and other statutory requirements.

Mass Digitization of Cultural Heritage: Can Copyright Obstacles Be Overcome?

http://livestream.com/unc-sils/iPres-Pamela-Samuelson/videos

Keynote presentation from iPRES 2015 by Pamela Samuelson, professor of Law and Information at the University of California, Berkeley. Samuelson has published extensively on IPR and Cyberlaw. In this presentation she considers the role of "fair use" in approaching the challenge that Copyright pose. Samuelson speaks from a US legal perspective but many considerations are also applicable in the UK context. (2015) 56 minutes

iPresKeynote

http://livestream.com/unc-sils/iPres-Pamela-Samuelson

References

Charlesworth, A.J., 2012. Intellectual Property Rights for Digital Preservation, *DPC Technology Watch Report 12-02*. Available: http://dx.doi.org/10.7207/twr12-02

Intellectual Property Office, 2014. *Exceptions to Copyright: Libraries, Archives and Museums*. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/375956/Libraries_Archives_and_Museums.pdf

Koops, B., 2011. *Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right To Be Forgotten" In Big Data Practice*. SCRIPTed, 8:3, 229-256. Available:http://script-ed.org/wp-content/uploads/2011/12/koops.pdf

Milligan, I., 2015. *Web Archive Legal Deposit: A Double-Edged Sword*. Available: http://ianmilligan.ca/2015/07/14/web-archive-legal-deposit-a-double-edged-sword/

Risk and Change Management

Illustration by Jørgen Stamp digitalbevaring.dk CC BY 2.5 Denmark

Introduction

Digital preservation is not simply about risks. It also creates opportunities and by protecting digital materials it means that new or extended value can be derived from them. It can be easy to become overwhelmed with risks, so It is worth being explicit early in the process about what opportunities are being protected or created. There are many things that put your digital resources at risk including changes to your organisation or technology. If not managed, these risks will have a significant impact on your ability to carry out your digital preservation activities, wider business functions, or comply with legislation.

To manage digital preservation, you must understand your organisation's specific issues and risks. You can do this by undertaking a risk and opportunities assessment. The assessment will highlight specific risks to the continuity of your digital resources, and opportunities that can be realised from mitigating these risks.

Risk management

Experience shows that the risks facing digital resources are subtle and varied. They include, but are not limited to the following:

- Merger, closure, or transfer of functions between organisations.
- Changes in strategic direction or funding and the functions supported by an organisation.
- Major changes in individual leaders or experts.
- Breakdown of resource discovery data resulting in difficulty retrieving data.
- Loss of copyright or other legal information resulting in uncertainty over rights and obligations.

- Outsourcing with no consideration of future preservation needs.
- File format obsolescence meaning that it is expensive or impossible to process data.
- Media obsolescence making it expensive or impossible to recover data.
- Media degradation meaning that data is damaged or changed.
- Loss of contextual information resulting in loss of meaning.
- Loss of provenance information or fixity about a document resulting in loss of authenticity.
- Breakdown of version control making it hard to identify authoritative instances of a document.
- Human error leading to accidental deletion.
- The degree of use. A dark archive is more at risk than one than is heavily used. If digital material is accessed infrequently the impact of failure is less immediately apparent.
- Natural Disasters affecting buildings or infrastructure.

Data loss is likely to have a variety of real world consequences depending on context. In the context of a court case, for example, the authenticity of a document could become a significant legal issue; whereas for highly structured research data the chain of custody may matter less than access to explanatory context that enables the reproducibility of an experiment. In many contexts it may be technically possible to recover digital collections but where an organisation simply doesn't have the wherewithal or skills necessary to restore a data set, then practical obsolescence and data loss can result. This is likely to become more of a reality as the number and complexity of digital collections expand.

The risks to digital content usually matter because of their consequences in the real world. Again this depends on the context but the following can occur:

- Loss of reputation.
- Inadequate resources for a critical task.
- Inability to support users in their activities.
- Failure to discharge legal or regulatory function.
- Inability to exploit and reuse data.
- Loss of identity and corporate memory.
- Cost of recreation and recovery.

Risks are typically prioritised by calculating a 'risk score' based on likelihood, impact and imminence: an imminent risk with a strong probability and a large negative impact needs prompt action. Depending on the nature of the risk this might include taking steps to reduce the likelihood of a risk emerging, reducing the impact if a risk does occur, or buying time for mitigation steps to be implemented.

Risk assessment is an ongoing process that can be developed and expanded through time. It can help bring together different stakeholders and, because risk management is understood by senior management it can also help to make the case for investment. Even an elementary risk assessment will highlight priorities for anyone getting started in digital preservation.

Finally it is worth noting that digital preservation is distinctive in being long-term and most risk methodologies are typically focussed on the short-term. For digital preservation, you need to be aware that over the long term improbable events will become more likely and special attention should be paid to those with significant consequences.

Business continuity planning

Rationale

'Interested parties and stakeholders require that organizations proactively prepare for potential incidents and disruptions in order to avoid suspension of critical operations and services, or if operations and services are disrupted, that they resume operations and services as rapidly as required by those who depend on them.' (ISO/PAS 22399:2007).

Business Continuity planning and practice is well-established within the IT profession and is not dealt with in detail in the Handbook. However it is an important component of ensuring bit preservation and makes a significant contribution to digital preservation through this. There is a series of webinars on business continuity and digital preservation from the TIMBUS project (see Resources).

The development and use of a business continuity plan based on sound principles, endorsed by senior management, and activated by trained staff will greatly reduce the likelihood and severity of impact of disasters and incidents.

One model is the plan developed by the Data Archive, and described in the DPC Case note on Business Continuity. Organisations may also wish to consider use of cloud services (see Cloud services) as part of their planning.

Requirements

- Develop a business continuity plan.
- Ensure all relevant staff are trained in business continuity procedures.
- Create copies of data resources at the time of their transfer to the institution.
- Store copies on industry standard or other approved contemporary media.
- Store copies on and off site. Off-site copies should be stored at a safe distance from on-site copies to ensure they are unaffected by any natural or man-made disaster affecting the on-site copies.
- Consider data and skills as assets and compile registers of them.
- Ensure roles and responsibilities are identified and maintained.

Resources

ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management

http://www.iso.org/iso/catalogue_detail?csnumber=50295

This standard provides general guidance for any organization to develop its own specific performance criteria for incident preparedness and operational continuity, and design an appropriate management system.

ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements

http://www.iso.org/iso/catalogue_detail?csnumber=54534

This standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system. The requirements are generic and are intended to be applicable to all organizations.

Disaster Preparedness for Digital Content

http://dpworkshop.org/workshops/management-tools/disaster-preparedness

A Digital Preservation Management workshop webpage that links a set of 4 suggested documents (disaster plan policy, communications plan, training plan, roles and responsibilities). Cumulatively they provide comprehensive documentation and are updated to reflect current practice for disaster preparedness.

National Archives Risk assessment tools

http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/risk-assessment/

The National Archives provide two excel format self-assessment tools that link to its digital continuity guidance and framework of solutions and services.

The Self-assessment tool (0.4 Mb) divides the risk assessment into three sections: Understanding digital continuity and roles and responsibilities; Information requirements and technical dependencies, and Management

The Information asset risk assessment tool (0.26 Mb) helps you identify risks to the continuity of any specific digital information asset and identifies where continuity has already been lost. It makes recommendations on maintaining or restoring continuity to help you develop a digital continuity action plan.

DRAMBORA (Digital Repository Audit Method Based on Risk Assessment) Toolkit

http://www.repositoryaudit.eu

This is an online toolkit for a digital repository audit. The toolkit guides users through the audit process, from defining the purpose and scope of the audit to identifying and addressing risks to the repository. DRAMBORA provides a list of over 80 examples of potential risks to digital repositories, framed in terms of possible consequences.

SPOT

http://www.dlib.org/dlib/september12/vermaaten/09vermaaten.html

The SPOT (Simple Property-Oriented Threat) provides a simple model for risk assessment, focused on safeguarding against threats to six properties of digital objects fundamental to their preservation: availability, identity, persistence, renderability, understandability, and authenticity. The model discusses threats in terms of their potential impacts on these properties, providing several example outcomes for each. The article describing the model also included a useful comparison of other digital preservation threat models.

Managing digital continuity guidance from The National Archives

http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/

Includes a helpful risk assessment with many correlations to risk management strategies for Business Continuity Planning.

Assess and manage risks to digital continuity

http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/step-by-step-guidance/step-3/

The National Archives have built a self-assessment tool for the wider public sector that links to its digital continuity guidance and framework of solutions and services.

Assess risks to digital continuity factsheet

http://www.nationalarchives.gov.uk/documents/information-management/assess-dc-risks-factsheet.pdf

(2 pages)

Risk assessment handbook

http://www.nationalarchives.gov.uk/documents/information-management/Risk-Assessment-Handbook.pdf

(35 pages)

The Atlas of Digital Damages

https://www.flickr.com/groups/2121762@N23/

This is a staging area for collecting visual examples of digital preservation challenges, failed renderings, encoding damage, corrupt data, and visual evidence documenting #FAILs of any stripe. You can contribute just an image, tell the story behind the image, or share the original file (or set of files), so that tool developers can learn from digital damage and test out their code with it.

TIMBUS project: Business Continuity Management 1 - Intro, Life Cycle, Planning, Scope

https://www.youtube.com/watch?v=25EhtuE3XkE

1 of 4 Business Continuity Management and the Digital Preservation of Processes webinars from the EU-funded Timbus project. This introduction is probably the most accessible for novices (released 2013. 13 mins).

Case studies

DPC case note: Business continuity procedures – UK Data Archive, University of Essex

http://www.dpconline.org/advice/case-notes/1562-case-note-business-continuity

The Data Archive is the UK national data centre for the Social Sciences funded by the Economic and Social Research Council (ESRC). The Archive holds certification to ISO 27001, the international standard for information security, which requires information security continuity to be embedded in an organisation's business continuity management systems. The digital storage system at the Data Archive is based, for security purposes, on segregated and distributed storage and access. Business continuity at the Data Archive is based around the resilience provided by creating multiple copies of the data and specified recovery procedures, alongside pre-emptive failure prevention. Each file from any dataset has at minimum three copies. The Archive also creates a read only archival copy of each study and any update as it is made available on the system.

References

ISO, 2007. *ISO/PAS 22399:2007. Societal security - Guideline for incident preparedness and operational continuity management.* Available: http://www.iso.org/iso/catalogue_detail?csnumber=50295

Staff Training and Development

Illustration by Jørgen Stamp digitalbevaring.dk CC BY 2.5 Denmark

Introduction

A well-skilled and effective workforce can be an organisation's greatest asset, yet due care and attention is not always given to providing adequate training and development, and encouraging its uptake. Additionally, developing and maintaining a digital preservation programme can seem daunting in many ways and, in particular, this is often due to a perceived staff skills gap. This may be because the work environment is characterised by:

- Rapid and ongoing change.
- Blurring of boundaries within and between institutions.
- Uncertainty in terms of the ability to confidently predict future trends and requirements.
- Unclear and/or changing roles and responsibilities.
- Increased emphasis on collaboration and teamwork.
- Increased emphasis on accountability.

Carefully designed staff training and continuous professional development (CPD) activities can play a key role in successfully making the transition from the traditional model of libraries and archives to the digital or hybrid model. Intelligent training and development can do much to boost confidence and ability in staff members, and minimise anxiety about the changing nature of work in preservation-performing institutions. A thoughtful approach to training and development (as opposed to just "sending people on courses") is likely to make a significant difference by:

- Helping staff to exploit technology effectively and improve the overall quality of service.
- Enhancing the individual level of job satisfaction and commitment, leading to improved staff retention.
- Improving the strategic outlook for the organisation as a whole.

Organisations should take a strategic approach to training and development, considering carefully the skills that are required, as well as new and developing roles and responsibilities. The issue should

be clearly addressed in all relevant digital preservation policy, strategy and planning, and budget for advocacy and skills development activities should be an integral part of planning for digital preservation work.

A Broad Range of Skills

Successful digital preservation work requires a broad range of skills, from those specific to the area such as knowledge of metadata standards and audit frameworks, to more general skills such a project planning and risk management. Therefore, ensuring all staff members have adequate digital preservation-specific skills for their part of the process is only one aspect of the preparation required for equipping them to maximise the potential of digital technology. It is highly unlikely that one individual will ever possess all of the skills required to undertake the full range of digital preservation activities, so collaboration will remain key to success. Skilful training can enhance individual skills and competences but can also enhance understanding of the other skills and competences required for a successful collaborative project.

A number of different initiatives have endeavoured to clarify the skills and competencies required for digital preservation work and potential roles involved for staff at different levels of seniority:

DPOE

The Library of Congress's Digital Preservation Outreach and Education programme (DPOE) has defined three levels of staff roles (or career stages) within their model for digital preservation training. These are:

- **Executive** - those in senior institutional management roles.
- **Managerial** - those managing digital preservation programmes and service.
- **Practical** - practitioners working hands-on with digital materials and preservation solutions.

DigCurV

The DigCurV project adapted the DPOE's three level model for their work in defining the core competencies required for digital preservation work. The DigCurV project examined a number of issues relating to digital curation and preservation training, skills and development, producing a variety of useful resources including a database of available training opportunities and a curriculum framework. Describing the core competencies required at each of the three levels in the DPOE model through a set of 'lenses', the DigCurV curriculum framework provides an excellent resource for those looking to identify the full range of skills and competencies required for digital curation and preservation. Specifically, the DigCurV curriculum framework can help users to describe and compare training courses, to develop new training resources and to map the skills and knowledge of an individual or team to identify any existing skills gaps.

Each lens is split into four sections covering

- Knowledge and Intellectual Abilities
- Personal Qualities
- Professional Conduct
- Management and Quality Assurance

Each then contain further sub-sections that list general statements about individual competencies. The statements are designed to be generic so have a broad applicability, although specific examples of particular standards or tools relating to the competencies are available via the version on the DigCurV website.

DigCCurr

The DigCCurr (Preserving Access to Our Digital Future: Building an International Digital Curation Curriculum) project has produced a 6-dimensional matrix for identifying and organizing the material to be covered in a digital curation curriculum. This Matrix of Digital Curation Knowledge and Competencies is an alternative approach that may be particularly useful for smaller organisations.

Roles and Responsibilities for Training and Development

Roles and responsibilities need to be clearly defined. The success of training and development programmes will be affected by the degree to which various roles and responsibilities mesh. It is essential that each of the stakeholders in the process fully appreciate their roles and actively participate in the process. Listed below is a guide to the various responsibilities that may be required of different stakeholders to ensure the creation and deployment of a successful and comprehensive training and development programme.

Stakeholder roles and responsibilities
Roles and Responsibilities of the Institution • Developing an Information Strategy which integrates IT training with the overall mission of the institution. • Identifying, in consultation with key staff, a skills audit, to determine what specific competencies are required to meet organisational objectives, including horizon-scanning for new and emerging skills, activities and responsibilities. • Establishing a balance between recruiting specific skills and effectively developing existing talent. • Providing adequate resources for training and development. • Ensuring staff have access to appropriate equipment. • Ensuring access to practical "hands on" training and practice. • Encouraging networking between colleagues in other institutions. • Considering strategies such as short-term secondment to an institution which may have more experience in a specific area. • Involving staff in designing training and development programmes. • Facilitating effective multidisciplinary communication. • Taking a broad view of what constitutes training and development (i.e. combination of formal courses, both generic and tailor-made, informal training within the organisation, skills transfer within the organisation, networking etc.).
Roles and Responsibilities of Professional Associations

- Responsiveness to current training and development needs.
- Ability to work with institutions to develop training packages to meet their needs.

Roles and Responsibilities of the Individual

- Ability to tolerate frequent change.
- Ability to be flexible.
- Ability to work in teams.
- Ability to communicate (including listening) effectively across staff groups and upwards / downwards within the organisation.
- Ability actively to pursue personal professional development through a range of mechanisms.
- Ability to share skills and expertise.
- Ability to learn new skills.
- Ability to apply new skills.

Undertaking a Skills Audit

A useful starting point for any organisation is to conduct a skills audit tailored to the needs of the specific institution. The process will help identify any skills gaps that exist and allow informed decisions to be made about training and development, as well as potentially highlighting additional roles that may require new staff or new responsibilities (and new job descriptions) for those already in post. Evidence from the skills audit can then be used to build a business case for any additional resources that may be required. In addition to being an excellent starting point for improving staff development it may also be useful to incorporate elements of the process into regular staff professional development and review processes.

The DigCurV curriculum framework or the Matrix of Digital Curation Knowledge and Competencies can provide a useful tool when carrying out a skills audit, in this case as a resource for benchmarking. It will be necessary to tailor the audit to the staff development practices and processes of individual organisations but the following steps may be considered:

1. Identify all roles within the organisation with digital preservation responsibilities. Examining workflows can help in this process and mapping these to models such as the OAIS Reference Model or the Digital Curation Centre Curation Lifecycle Model.
2. Map roles to the relevant lenses of the DigCurV framework.
3. Work with role holders to map skills to the relevant lens. This can be done variety of ways including self-assessment and as a group activity. It may also be useful to mark on a scale.
4. Analyse results to identify gaps, training requirements and additional roles required.

Training and Development Options

A lack of established training and development opportunities was previously a considerable barrier to those wishing to learn more about digital preservation. While those at more advanced levels in

their development may still struggle to find appropriate opportunities, there are now a number of established courses available to those at a beginner and intermediate level from short courses to full degree programmes including a variety of training opportunities addressing specific specialist areas of interest. A greater barrier is now the time and expense involved in attending face-to-face training, but increasingly more online and distance learning options are being made available so this impediment will also decrease.

Digital preservation courses have also previously suffered from criticism relating to an emphasis on theory rather than practice. This too is changing with more practical exercises and tool demos being incorporated into training. Digital preservation also remains a discipline where as much, if not more, can be learnt by doing, so peer to peer learning and a willingness to just get your hands dirty can often produce the best results. Information sharing and short staff exchanges with similar organisations can provide a particularly effect method for staff development and learning.

Resources

APARSEN Survey for the Assessment of Training Material/Assessment of Digital Curation Requirements

http://www.alliancepermanentaccess.org/wp-content/uploads/downloads/2012/12/APARSEN-REP-D43_1-01-4_1.pdf

This report presents the findings of research undertaken to in order to set the objectives and strategies for the development of training courses for digital preservation practitioners within the Network of Excellence. The aim of the research was to draw together a comprehensive picture of the digital preservation training that was then available and to identify the training needs of practitioners working within the field. (2012, 109 pages).

2014 DPOE Training Needs Assessment Survey

http://www.digitalpreservation.gov/education/2014_Survey_Report-Final.pdf

An analysis of the state of digital preservation practice and the capacity to preserve digital content within organisations in the United States with the aim of establishing training gaps and needs. (13 pages).

DigCurV, A Curriculum Framework for Digital Curation

http://www.digcurv.gla.ac.uk/

The DigCurV Curriculum Framework offers a means to identify, evaluate, and plan training to meet the skill requirements of staff engaged in digital curation. The DigCurV team undertook multi-national research in the Cultural Heritage sector to understand the skills used by those working in

digital curation, and those sought by employers in this sector. The framework defines separate skills lenses to match the specific needs of three distinct audiences; Executives, Managers, and Practitioners.

- The skills defined under the **Executive Lens** enable a digital curation professional to maintain a strategic view .
- The skills defined under the **Manager Lens** enable a professional to plan and monitor execution of digital curation projects, to recruit and support project teams, and to liaise with a range of internal and external contacts within the cultural heritage sector.
- The skills defined under the **Practitioner Lens** enable a professional to plan and execute a variety of technical tasks, both individually and as part of a multi-disciplinary team.

Matrix of Digital Curation Knowledge and Competencies

http://ils.unc.edu/digccurr/digccurr-matrix.html

The DigCCurr (Preserving Access to Our Digital Future: Building an International Digital Curation Curriculum) project has produced a 6-dimensional matrix for identifying and organizing the material to be covered in a digital curation curriculum.

Digital Preservation Outreach and Education

http://www.digitalpreservation.gov/education/curriculum.html

The Library of Congress's 'baseline' digital preservation training programme for archives and collections management staff. The full course is delivered to archives and other digital preservation professionals in a 'train the trainer' approach, in order to support further dissemination to colleagues. The overview videos are available online.

DPC Training

http://www.dpconline.org/training

A key role for the DPC is to empower and develop its members' workforces. The DPC addresses this issue by facilitating training and support activities and creating practitioner-focused material and events throughout each year. These include The DPC Leadership Programme, The Digital Preservation Roadshow, and The Member Briefing Days and Invitational Events.

Digital Preservation Training Programme (DPTP)

http://dptp.org

A range of UK based digital preservation training courses. Scheduled DPTP courses run over 2 days or 3 days and take place regularly throughout the year.

Digital Preservation Management: Implementing Short-Term Strategies for Long-Term Solutions

http://www.dpworkshop.org/

An excellent free online tutorial that introduces you to the basic tenets of digital preservation. It is particularly geared toward librarians, archivists, curators, managers, and technical specialists. It includes definitions, key concepts, practical advice, exercises, and up-to-date references. The tutorial is available in English, French, and Italian.

UK University post-graduate degree courses

http://www.dpconline.org/training/relevantpostgrads

The DPC maintains a list that will be helpful to anyone looking at post- graduate degrees with a focus on digital preservation. It includes University on campus and distance learning options. Some universities also offer individual credit bearing modules in relevant digital preservation topics.

Education and Training in Audio-visual Archiving and Preservation

http://www.arsc-audio.org/etresources.html

Training opportunities in Australia, Europe and the USA for those working with sound and moving image material.

Connecting to Collections: Caring for Audio-visual Material

http://www.connectingtocollections.org/av/

Self-paced course including recorded webinars, hand-outs, slideshows and suggested further reading for the individual student working with audio-visual material. It covers basic principles, a history of formats and their preservation challenges, format identification, access issues and an overview of existing models and standards. It is written in English by a team of US-based archivists, conservators and digital preservation experts.

How the DPC makes a difference to your staff

https://vimeo.com/45433968

Short interviews with 5 candidates who were sponsored by the Digital Preservation Coalition to attend the Digital Futures Academy in London in March 2012. They reflect on their experience and how joining the DPC has benefitted their institutions. (2 mins 40 secs)

Standards and Best Practice

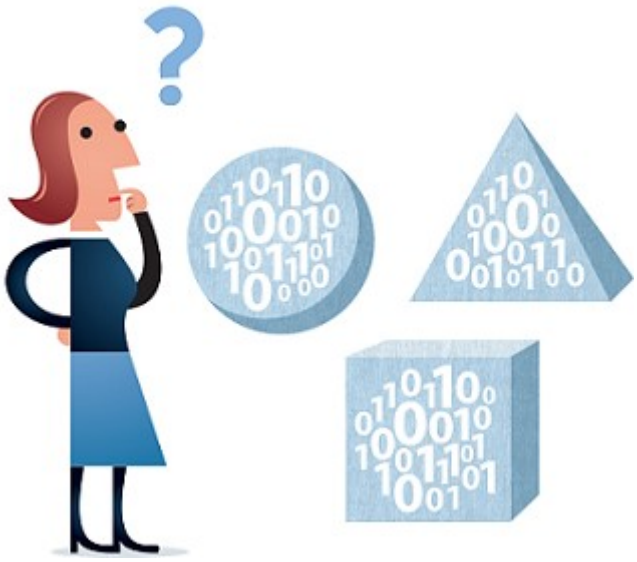


Illustration by Jørgen Stamp digitalbevaring.dk CC BY 2.5 Denmark

Introduction

The use and development of reliable standards has long been a cornerstone of the information industry. They facilitate the access, discovery and sharing of digital resources, as well as their long-term preservation. There are both generic standards applicable to all sectors that can support digital preservation, and industry-specific standards that may need to be adhered to. Using standards that are relevant to the digital institutional environment helps with organisational compliance and interoperability between diverse systems within and beyond the sector. Adherence to standards also enables organisations to be audited and certified.

Operational standards

There are a number of standards which can help with the development of an operational model for digital preservation.

Taking custodial control of digital materials requires a set of procedures to govern their transfer into a digital preservation environment. This can include identifying and quantifying the materials to be transferred, assessing the costs of preserving them and identifying the requirements for future authentication and confidentiality. ISO 20652: Space Data and Information Transfer Systems - Producer-Archive Interface - Methodology Abstract Standard (ISO, 2006) is an international standard that provides a methodological framework for developing procedures for the formal transfer of digital materials from the creator into the digital preservation environment. Objectives, actions and the expected results are identified for four phases - initial negotiations with the creator (Preliminary Phase), defining requirements (Formal Definition Phase), the transfer of digital materials to the digital preservation environment (Transfer Phase) and ensuring the digital materials and their accompanying metadata conform to what was agreed (Validation Phase).

ISO 14721:2012 Space Data and Information Transfer Systems - Open Archival Information System - Reference Model (OAIS) (ISO, 2012b) provides a systematic framework for understanding and implementing the archival concepts needed for long-term digital information preservation and access, and for describing and comparing architectures and operations of existing and future archives. It describes roles, processes and methods for long-term preservation. Developed by the

Consultative Committee for Space Data Systems (CCSDS) OAIS was first published in 1999 and has had an influence upon many digital preservation developments since the early 2000s. A useful introductory guide to the standard is available as a DPC Technology Watch Report (Lavoie, 2014).

An OAIS is 'an archive, consisting of an organization of people and systems that has accepted the responsibility to preserve information and make it available for a defined 'Designated Community'. An 'OAIS archive' could be distinguished from other uses of the term 'archive' by the way that it accepts and responds to a series of specific responsibilities. OAIS defines these responsibilities as:

- Negotiate for and accept appropriate information from information producers;
- Obtain sufficient control of the information in order to meet long-term preservation objectives;
- Determine the scope of the archive's user community;
- Ensure that the preserved information is independently understandable to the user community, in the sense that the information can be understood by users without the assistance of the information producer;
- Follow documented policies and procedures to ensure the information is preserved against all reasonable contingencies, and that there are no ad hoc deletions.
- Make the preserved information available to the user community, and enable dissemination of authenticated copies of the preserved information in its original form, or in a form traceable to the original. (Lavoie, 2014)

OAIS also defines the information model that needs to be adopted. This includes not only the digital material but also any metadata used to describe or manage the material and any other supporting information called Representation Information.

The OAIS functional model is widely used to establish workflows and technical implementations. It defines a broad range of digital preservation functions including ingest, access, archival storage, preservation planning, data management and administration. These provide a common set of concepts and definitions that can assist discussion across sectors and professional groups and facilitate the specification of archives and digital preservation systems.

OAIS provides a high level framework and a useful shared language for digital preservation but for many years the concept of 'OAIS conformance/compliance' remained hard to pin down. Though the term was frequently used in the years immediately following the publication of the standard, it relied on the ability to measure up to just six mandatory but high level responsibilities. A more detailed discussion about 'OAIS compliance' can be found in the Technology Watch Report.

ISO/TR 18492:2005 Long-term preservation of electronic document-based information (ISO/TR, 2005) provides a practical methodology for the continued preservation and retrieval of authentic electronic document-based information, which includes technology-neutral guidance on media renewal, migration, quality, security and environmental control. The guidance is developed to ensure authenticity of records beyond the lifetime of original information keeping systems.

ISO 15489:2001 Information and documentation -- Records management (ISO, 2001) can also be a useful standard for defining the roles, processes and methods for a digital preservation implementation where the focus is the long-term management of records. This standard outlines a

framework of best practice for managing business records to ensure that they are curated and documented throughout their lifecycle while remaining authoritative and accessible.

ISO 16175:2011 Principles and functional requirements for records in electronic office environments (ISO, 2011) relates to electronic document and records management systems as well as enterprise content management systems. While it does not include specific requirements for digital preservation, it does acknowledge the need to maintain records over time and that format obsolescence issues need to be considered in the specification of these electronic systems.

There are international standards that are generic to good business management that may also be relevant in the digital preservation domain.

- Certification against ISO 9001 Quality management systems (ISO, 2015) demonstrates an organisation's ability to provide and improve consistent products and services.
- Certification against ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems (ISO/IEC, 2013) demonstrates that digital materials are securely managed ensuring their authenticity, reliability and usability.
- ISO/IEC 15408 The Common Criteria for Information Technology Security Evaluation (ISO/IEC, 2009) provides a standardised framework for specifying functional and assurance requirements for IT security and a rigorous evaluation of these.

There are a number of routes through which a digital preservation implementation can be certified. These range from light touch peer review certification methods such as the Data Seal of Approval, through the more extensive internal methods of DIN 31644 Information and documentation - Criteria for trustworthy digital archives (DIN, 2012), to the comprehensive international standard ISO 16363:2012 Audit and certification of trustworthy digital repositories (ISO, 2012a) (see Audit and certification).

Technical standards

There are specific advantages to using standards for the technical aspects of a digital preservation programme, primarily in relation to metadata and file formats.

In conjunction with relevant descriptive metadata standards, PREMIS and METS are de facto standards which will enhance a digital preservation programme. PREMIS (PREservation Metadata: Implementation Strategies) is a standard hosted by the Library of Congress and first published in 2005. The data dictionary and supporting tools have been specifically developed to support the preservation of digital material. METS (Metadata Encoding and Transmission Standard) is an XML encoding standard which enables digital materials to be packaged with archival information (see Metadata and documentation).

There are also standards relating to file formats. Choosing file formats that are non-proprietary and based on open format standards gives an organisation a good basis for a digital preservation programme. ISO/IEC 26300-1:2015 Open Document Format for Office Applications (ISO/IEC, 2015) provides an XML schema for the preservation of widely used documents such as text documents, spreadsheets, presentations. ISO 19005 Electronic document file format for long-term preservation (ISO, 2005) prescribes elements of valid PDF/A which ensures that they are self-contained and display consistently across different devices. Aspects of **JPEG-2000** and **TIFF** are also covered by ISO standards. (see File formats and standards).

Barriers to using standards

A standards based approach to digital preservation is important, but there are also factors which inhibit their use as a digital preservation strategy:

- The pace of change is so rapid that standards which have reached the stage of being formally endorsed - a process which usually takes years - will inevitably lag behind developments and may even be superseded.
- Competitive pressures between suppliers encourage the development of proprietary extensions to, or implementations of standards which can dilute the advantages of consistency and interoperability for preservation.
- The standards themselves adapt and change to new technological environments, leading to a number of variations of the original standard which may or may not be interoperable in the long-term even if they are backwards compatible in the short-term.
- Standards can be intimidating to read and resource intensive to implement.
- In such a changeable and highly distributed environment, it is impossible to be completely prescriptive.

These factors mean that standards will need to be seen as part of a suite of preservation strategies rather than the key strategy itself. The digital environment is not inclined to be constrained by rigid rules and a digital preservation programme can often be a blend of standards and best practice that is sufficiently flexible and adapted to suit the needs of the organisation, its circumstances and the digital materials being managed.

Standards, best practice and good practice

In recent years best practice guidance and case studies have been published by national archives, national libraries and other cultural organisations. Digital preservation is also a topic well discussed on blogs and social media which can often provide real time information in relation to theory and practice from around the world. Papers at conferences such as iPRES, the International Digital Curation Conference (IDCC) and the Preservation and Archiving Special Interest Group (PASIG) can be a useful source of up to date thinking from academics and practitioners in digital preservation.

Standards should be understood as a formal description and recognition of what a community of experts might term best practice. Standards, and the best practice from which they derive can be intimidating and there is a risk for those starting in digital preservation that the 'best becomes the enemy of the good'. So in adopting or recommending standards it should always be understood that some action is almost always better than no action. Digital preservation is a messy business which throws up unexpected challenges. So it is almost always the case that a poorly implemented standard is preferable to waiting for perfection.

Sector specific requirements

Specific industries have become active in the development of preservation standards, and particular types of content and use cases have emerged that overlap and extend a number of standards. There is considerable benefit in digital preservation standards being embedded in sector-specific standards since this will greatly assist their adoption, although this may present a challenge to coordination of activities. Three examples are given below:

1. Audio visual materials present a special case for digital preservation (see Moving pictures and sounds). Recommendations for audio recordings and video recordings exist under the

auspices of the International Association of Sound and Audio-visual Archives (such as IASA-TC04, 2009), while a range of industry bodies and content holders including the BBC, RAI, ORF and INA have formed the PrestoCentre to progress research and development of preservation standards in this field. https://www.prestocentre.org/

2. The aerospace industry has particular requirements in product lifecycle management and information exchange which have given rise to a series of industry wide initiatives to standardise approaches to aligning and sharing CAD drawings for engineering. The membership body PROSTEP created the ISO 10303 'Standard for Exchange of Product Model Data' which has developed into the LOTAR standard (http://www.lotar-international.org/lotar-standard/overview-on-parts.html). LOTAR is not incompatible with OAIS, but because it fits within a data exchange protocol important to the industry, aerospace engineers are more likely to encounter LOTAR than OAIS

3. .The Storage Network Industry Association has also begun to make progress on the development of a series of standards. A SNIA working group on long-term data retention has responsibility for both physical and logical preservation, and the creation of reference architectures, services and interfaces for preservation. In addition, a working group on Cloud Storage is likely to become particularly influential in relation to preservation. Cloud architectures change how organizations view repositories and how they access services to manage them. For example, it is unclear how one would measure the success of a 'trusted digital repository' that was based in a cloud provider.

Resources

Seeing Standards; A visualisation of the metadata universe

http://www.dlib.indiana.edu/~jenlrile/metadatamap/seeingstandards.pdf

The sheer number of metadata standards in the cultural heritage sector is overwhelming, and their inter-relationships further complicate the situation. This visual map of the metadata landscape is intended to assist planners with the selection and implementation of metadata standards. Each of the 105 standards listed here is evaluated on its strength of application to defined categories in each of four axes: community, domain, function, and purpose. (2010, 1 page).

Dlib Magazine

http://www.dlib.org/dlib.html

Dlib Magazine publishes on a regular basis a wide range of papers and case studies on the practical implementation of digital preservation standards and best practice.

Data Seal of Approval

http://datasealofapproval.org/en/

PREMIS

http://www.loc.gov/standards/premis/

Library of Congress, 2015

The Digital Curation Centre

http://www.dcc.ac.uk/

The Digital Curation Centre makes available research and case studies in relation to the preservation of research data. Iit also publishes recordings of its annual international digital curation conference proceedings.

The Signal

http://blogs.loc.gov/digitalpreservation/

The Signal is a digital preservation blog published by the Library of Congress

IPRES

http://www.ipres-conference.org/

IPRES, the International Conference on Digital Preservation publishes a website and proceedings from their annual event which looks at different themes within the digital preservation landscape,

The Digital Preservation Coalition Wiki

http://wiki.dpconline.org/index.php?title=Main_Page

The Digital Preservation Coalition Wiki provides a collaborative space for users of OAIS, the British Library's file format assessments as well as other resources.

Digital Preservation Matters

http://preservationmatters.blogspot.co.uk/

The Digital Preservation Matters blog is a personal account of experiences from working with Digital Preservation

References

DIN, 2012. *DIN 31644 Information and documentation - Criteria for trustworthy digital archives*. Available: http://data-archive.ac.uk/curate/trusted-digital-repositories/standards-of-trust?index=3

IASA-TC04, 2009. *Guidelines in the Production and Preservation of Digital Audio Objects: standards, recommended practices, and strategies: 2nd edition,* edited by Kevin Bradley. Available: http://www.iasa-web.org/tc04/publication-information

ISO, 2001. *ISO 15489:2001 Information and documentation -- Records management*. Geneva: International Organization for Standardization. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=31908

ISO, 2005. *ISO 19005-1:2005. Document management -- Electronic document file format for long-term preservation*. Geneva: International Organization for Standardization. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=38920

ISO, 2006. *ISO 20652:2006 Space Data and Information Transfer Systems - Producer-Archive Interface - Methodology Abstract Standard*. Geneva: International Organization for Standardization. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39577

ISO, 2011. *ISO 16175:2011 Principles and functional requirements for records in electronic office environments.* Geneva: International Organization for Standardization. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=55791

ISO, 2012a. *ISO 16363:2012 Audit and certification of trustworthy digital repositories.* Geneva: International Organization for Standardization. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56510

ISO, 2012b. *ISO 14721:2012 Space Data and Information Transfer Systems - Open Archival Information System (OAIS) - Reference Model.* Geneva: International Organization for Standardization. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=57284

ISO, 2015. *ISO 9001:2015 Quality management systems. Geneva: International Organization for Standardization*. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62085

ISO/IEC, 2009. *ISO/IEC 15408:2009 The Common Criteria for Information Technology Security Evaluation*. Geneva: International Organization for Standardization. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50341

ISO/IEC, 2013. *ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems*. Geneva: International Organization for Standardization. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

ISO/IEC, 2015. *ISO/IEC 26300-1:2015 Information technology -- Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 1: OpenDocument Schema*. Geneva: International Organization for Standardization. Available:http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=66363

ISO/TR, 2005. *ISO/TR 18492:2005 Long-term preservation of electronic document-based information*. Geneva: International Organization for Standardization. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=38716

Lavoie, B., 2014. The Open Archival Information System (OAIS) Reference Model: Introductory Guide (2nd Edition). *DPC Technology Watch Report 14-02*. Available: http://dx.doi.org/10.7207/twr14-02

Library of Congress, 2015. *METS Metadata Encoding and Transmission Standard*. Available: http://www.loc.gov/standards/mets/

Business Cases, Benefits, Costs, and Impact

Illustration by Jørgen Stamp digitalbevaring.dk CC BY 2.5 Denmark

Introduction

Any change in the economic environment may mean that many organisations are challenged to reduce overall expenditure and to maximise efficiencies. At the same time organisations are preserving increasing amounts of digital material. Reuse of models can form a part of the response to this challenge. The long term management - preservation - of digital materials is an expensive and complex activity. It cannot reliably be done without the investment of resources and expenditure.

The challenges for an organisation are to create business models that:

- Can help define benefits and outcomes and convince key decision makers that it is a worthwhile endeavour;
- Support the wider aims and objectives of the parent organisation;
- Provide for the future of their digital materials in an economically sustainable way and helps reconcile the difference between short to mid-term funding commitments/funding cycles, and long-term preservation goals.

Other organisations have already created templates for business cases and models for the calculation of cost and benefit, so reusing some or parts of these models can not only save time but be used as justification for the adoption of particular strategies.

Business cases

The business case is a tool for advocating and ensuring that an investment is justified in terms of the strategic direction of the organisation and the benefits it will deliver. It typically provides context, benefits, costs and a set of options for key decision makers and funders. It can also set out how success will be measured to ensure that promised improvements are delivered.

It is essential that any business model or proposal that is created supports the wider aims and objectives of the parent organisation. It is equally important that key stakeholders, such as budget holders, are consulted and given early sight of the plans and offered the opportunity to comment and provide input. Early exposure of plans can to some extent mitigate situations in which plans might otherwise be rejected outright.

However, presenting a business case for preserving any material at an early stage is no guarantee that it will be accepted. Whilst there is no sure fire template, some or all of the following steps may be useful if a plan is rejected. Within an organisation there may be set procedures and policies regarding the making and presentation of business cases and these should be followed. Early communication of business planning can help identify topics or areas that could present problems when the plan is formally presented.

Identify options and be pragmatic

The point of business planning is to be aspirational and to create services or products that have value and benefit. Not everyone sees the benefits in preservation over the long term where costs are an ongoing issue or where resources are required to be committed for the long term. Business planning is often an exercise in pragmatism. It might be more effective to make a number of smaller more focussed business plans than one single large proposal. Using their knowledge of an organisation the author of a business plan must ensure that any plan is realistic and within the means of the organisation. Strategic planning provides the framework within which business plans are written. Any strategic objective can be achieved in a number of ways, e.g. less money but more time, fewer staff but longer timeframe etc. A pragmatic response offers decision makers a preferred option and why it is preferred and a small range of other alternative options in the business case. It is often helpful to include the "costs/dis-benefits of inaction" as an option against which other actions can be evaluated.

If at first you don't succeed

Work with stakeholders to identify reasons why a business plan was rejected. Talk to those involved in decision making and seek specific feedback. Was the cost component too expensive? Were the plans too ambitious? Is it felt the business case was poorly written or presented? Does the timeframe not fit with organisational plans?

Response: Work with stakeholders to address key concerns. Be clear to address each issue. Explain the reasons why a business plan was presented and what it is aiming to achieve. Focus on benefits, especially those that address the key strategic goals of the parent organisation. Focus on short as well as longer term benefits of the business plan. One approach is to create business plans that are 'SMART', that is Specific, Measurable, Achievable, Realistic and Timely.

When circumstances change

The hard work in business planning is getting to the point where a plan is accepted. However, circumstances can change. If a business plan is not implemented or previously agreed funding withdrawn, the implications can be severe. Again, communication with key stakeholders is essential and can reveal why something may have changed.

Response: Part of business planning involves having a range of options that can be offered in the event of problems arising with funding a preferred option. Having a well-structured business plan from which proposals can be deleted can help in making an alternative case for phased or alternative implementations requiring fewer resources. In such a case a business plan might quickly be re-drafted in more acceptable terms and resources made available. Having a focus on why resources were not made available gives an opportunity for a business case to be re-presented with more emphasis on benefits and positive impact.

Creating business cases

The following steps should be considered when writing and delivering a business case.

Creating a business case	
1. Audit your digital materials and prioritise work required	Audit your digital materials. Analyse the risks and opportunities for your digital materials. Use your analysis to prioritise areas of work and assign owners to them.
2. Is this the right time?	What are you already doing? Is it the right time to do new things on your own? Can you collaborate with others?
3. Institutional analysis	How ready is your institution for change in terms of content and process?
4. Stakeholder analysis and advocacy	Who will be working on and using the digital materials? Who decides on funding? Engage with them using language and terms they will understand.
5. Objectives: scope aims, activities, plan and costs	Map out what are you going to do, who will do what, what will it cost, and when it will happen.
6. Map benefits to organisational strategy	Make sure you express the benefits of your business case in a way that your funders will understand.
7. What else is needed?	Do you need to include a cost-benefits analysis or list of options based on expenditure and outcome?
8. Validate and refine business case	Review and test your business case against best practice and identify what else it needs.
9. Deliver the business case with maximum impact	Do you have a champion to use in the organisation? Remember you may need to deliver it again.
10. Share an edited business case	Remove confidential material and share online so others can benefit from your work

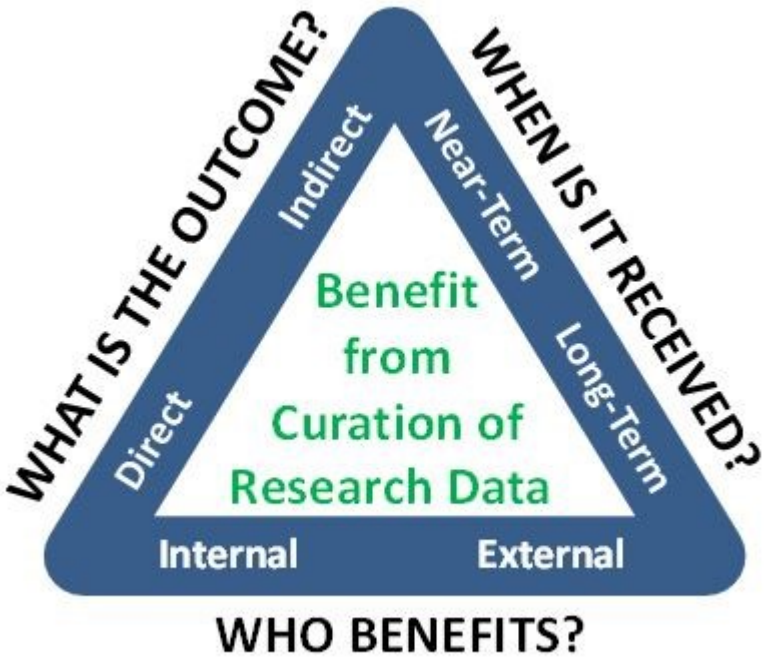
For a generic digital preservation business case template and more information, see the Digital Preservation Business Case Toolkit

Benefits

Benefits are associated with costs and also with risks (see Risk and change management). If risks are mitigated these become a type of benefit. The purpose of the acquisition of any digital material is that it is used. The uses to which digital material is put represents a benefit to those users. If an organisation needs to understand costs associated with digital materials then it must also understand benefits. Benefits can be used to justify costs through the development of business plans.

Measuring benefits is often quite challenging, especially when these benefits do not easily lend themselves to expression in quantitative terms. Often a mixture of approaches will be required to analyse both qualitative and quantitative outcomes and present the differences made. To assist

institutions, the Keeping Research Data Safe project created a KRDS Benefits Framework and a Benefits Analysis Toolkit (KRDS, 2011). These aim to help institutions identify the full scope of benefits from management and preservation of research data and to present them in a succinct way to a range of different stakeholders (e.g. when developing business cases or advocacy). The toolkit is also easily applicable to the benefits of digital preservation to other classes of digital materials.



The KRDS Benefits Framework uses three dimensions to illuminate the benefits investments potentially generate. These dimensions serve as a high-level framework within which thinking about benefits can be organised and then sharpened into more focused value propositions using the Toolkit. It helps you identify what changes you are trying to deliver, what are the outcomes, who benefits, and how long it will take to realise those benefits.

Costs

A business case will normally look at not just the establishment cost for the digital preservation solution, but the all-in cost, including project/program management costs and other activities being undertaken to support implementation such as training and publicity. However digital preservation costs are often the most critical element.

Why understand digital preservation costs?

These are a few reasons why an organisation might want to estimate digital preservation costs:

- Planning and budgeting to build a new repository from scratch, or to extend an existing one.
- Adding a new digital material to your repository and deciding if you can afford it now or over the long-term.
- Providing a platform for comparison with like organisations and an opportunity to adopt efficiencies that have been identified by others.
- Deciding whether to outsource activities or do it in-house.

- Deciding how much to charge for providing a digital preservation service to clients.
- Understanding where resources are being used or under-utilised and areas where additional allocation of resources might be beneficial.

What is lifecycle cost modelling?

A number of research and development projects have sought to model digital preservation costs across the lifecycle from creation and ingest through to preservation and ultimately access. The large number of projects makes understanding this work, finding which results are most applicable to a particular situation, choosing a model, and putting it into practice a significant challenge. The 4C Project surveyed, analysed and assessed this work and provides guidance on getting the most from it:

- Starting out with curation costs - provides an introduction to the concepts.
- Using cost models - describes how to select a cost model appropriate to your organisation.
- Cost Concept Model and Gateway Specification - provides more detail including a guide to develop a model to your own requirements looking at concepts such as 'risk', 'value', 'quality' and 'sustainability'.

Challenges with cost modelling

Cost modelling has been identified as a particularly challenging activity, with a number of difficult aspects, such as:

- Articulating the drivers or aims for costing digital preservation.
- Digital preservation is a moving target, defined by changing technologies and evolving institutional requirements.
- Level of detail: At a high level, modelling becomes less useful as it typically relates to a cross section of different preservation contexts. Modelling at a low level quickly becomes highly complex, making models difficult to develop, maintain and put into use.
- Organisations are reluctant to share costing data, with which models may be developed and validated.
- Even where costing data has been shared, it is often difficult to map between the different costing models it is associated with.
- Separating out digital preservation costs from other business costs is difficult and sometimes meaningless (example: digitising collections in a way that helps ingest into content into the preservation environment –is this digital preservation or digitisation costs?)

For this reason, modelling digital preservation costs across the lifecycle is an activity that should be approached with caution. Cost modelling will always be an approximation and so you need to decide the amount of time you are willing to put in to gain a less approximate answer.

Managing costs

It is possible to manage costs through careful planning. One way is through good process design. The ways in which digital material is created or acquired, managed and disseminated attract costs. Those costs are at the discretion of the organisation and can be managed. The end to end process from acquisition to dissemination must be designed to ensure that all activities are as efficient as possible.

All steps should be designed in such a way as to minimise the need for resources, whilst maximising efficiency. Whilst efficiencies work well at scale, an efficient process doesn't have to be a high volume process. Automation of systematic steps can also save time and deliver effective consistent processes. The initial costs of process design and implementation can be offset by longer term returns.

Impact

Impact is typically the measurement of benefits particularly to the wider public and society undertaken after a business case project has delivered.

For small projects and business cases, impact may be just a simple set of measures such as downloads or number of website requests against which success can be benchmarked easily.

For larger projects and programmes, it may be part of a more thorough evaluation to justify the resources expended. It can include a mixture of quantitative and qualitative measures and will normally be undertaken by external specialists working with staff from the repository. They employ methods from economics and management and information science, for example cost-benefit analysis or contingent valuation, and traditional social science methods such as interviews, surveys and focus groups.

Measurement involves choosing metrics or indicators and requires careful planning and agreement about what to measure and how. Metrics often employ readily countable things such as downloads, or scales metrics that are not truly numeric, such as rating scales or categories of variables. Typically there is a trade-off between what ideally should be measured (e.g. users and use) and proxy measures which are easy to capture and measure (e.g." unique visitors" and web downloads).

Resources

Sustainable Economics for a Digital Planet: Ensuring Long-Term Access to Digital Information

http://brtf.sdsc.edu/biblio/BRTF_Final_Report.pdf

The Blue Ribbon Task Force investigated sustainable digital preservation and access from an economic perspective. This final report, identifies problems intrinsic to all preserved digital materials, and proposes actions that stakeholders can take to meet these challenges to sustainability. It developed action agendas that are targeted to major stakeholder groups and to domain-specific preservation strategies. (2010, 116 pages).

The Value and Impact of Data Sharing and Curation: A synthesis of three recent studies of UK research data centres

http://repository.jisc.ac.uk/5568/1/iDF308_-_Digital_Infrastructure_Directions_Report%2C_Jan14_v1-04.pdf

This synthesis summarises and reflects on the combined findings from a series of independent investigations into the value and impact of three well established UK research data centres or services (the Economic and Social Data Service, the Archaeology Data Service, and the British Atmospheric Data Centre). The studies adopted a number of approaches to explore the value and

impacts of research data services and the data sharing and archiving that they have enabled. Data collection involved focused user and depositor surveys, and data centre financial and operational data (e.g. user registrations, dataset deposits and downloads), supplemented by in-depth interviews. Not all impacts can be captured and quantified; therefore they have used these economic approaches with others, such as the KRDS Benefits Framework, to illustrate wider benefits. (2014, 26 pages).

Jisc DigitalMedia infokit on Sustainability and Funding

http://www.jiscdigitalmedia.ac.uk/infokit/digitisation-funding-and-sustaina/digitisation-funding-and-sustaina-home

Provides a starting point for considering the issues necessary to create and build a business model that will support sustainability of digitisation and digital collections.

4C Project Collaboration to Clarify the Costs of Curation

http://4cproject.eu/

The European Union funded 4C project aimed to help organisations across Europe to invest more effectively in digital curation and preservation. A series of reports and resources were produced and are available from its outputs and deliverables page. These include the Digital Curation Sustainability Model , an Evaluation of Cost Models and Needs & Gaps Analysis, a Report on Risk, Benefit, Impact and Value, and a Draft Economic Sustainability Reference Model. The evaluation of costs models report evaluates ten available cost models including, KRDS and LIFE. Another major output was the Curation Costs Exchange (CCEx), a community owned platform which helps organisations of any kind assess the costs of curation practices through comparison and analysis. The CCEx aims to provide real information about costs to help make more informed investments in digital curation. The CCEx was launched in 2014 by 4C and is now maintained and governed by the Digital Preservation Coalition (DPC) with help from nestor and The Netherlands Coalition for Digital Preservation (NCDD).

Digital Preservation Business Case Toolkit

http://wiki.dpconline.org/index.php?title=Digital_Preservation_Business_Case_Toolkit

This Toolkit provides an in depth guide to writing a business case that is focused on digital preservation activities. It's targeted at practitioners (and their managers) who are working with digital resources and would like to obtain funds to expand their digital preservation activities. The Toolkit is primarily aimed at those seeking further funds from within their organisation, but could also provide useful information for those writing a bid for project funds from an external funding body. It includes a Step by step guide to building a business case and a Template for building a business case. Created by the Jisc funded SPRUCE Project in 2013 the toolkit wiki is hosted by the DPC.

Keeping Research Data Safe (KRDS) Benefits Toolkit

http://www.beagrie.com/krds/

Keeping Research Data Safe (KRDS) is a series of cost/benefit studies, tools and methodologies that focus on the challenges of assessing costs and benefits of curation and preservation of research data. Although focussing on research data, the tools are easily customised to apply to other areas of digital preservation. Available outputs include a KRDS Factsheet, a KRDS User Guide, a KRDS Activity Cost Model, and a KRDS Benefits Analysis Toolkit as well as supplementary materials and reports. The KRDS projects between 2008 and 2011 were funded by Jisc.

20 Cost Questions for Digital Preservation

http://www.metaarchive.org/public/publishing/ma_20costquestions_final.pdf?thumblink

The MetaArchive Cooperative has produced a set of 20 questions to "assist institutions with their comparative analysis of various digital preservation solutions". This work marks a move away from the development of detailed predictive costing models towards a more general approach that seeks to identify and understand key cost drivers rather than the actual costs themselves.

DSHR's Blog

http://blog.dshr.org/search/label/storage%20costs
http://blog.dshr.org/search/label/cloud%20economics

David Rosenthal is a frequent blogger on the topic of storage costs, often considering the impact of the evolution of storage technology on preservation costs and on cloud storage.

A Digital Asset Sustainability and Preservation Cost Bibliography

http://blogs.loc.gov/digitalpreservation/2012/06/a-digital-asset-sustainability-and-preservation-cost-bibliography/

A bibliography that "ranges broadly, from articles on "contingent valuation," "ecosystem valuation" and the general "costs" of knowledge, to those that directly address the cost issues associated with digital preservation and stewardship".

Digital Preservation and Data Curation Costing and Cost Modelling

http://wiki.opf-labs.org/display/CDP/Home

A list of digital preservation cost models and cost modelling initiatives.

The Cost of Inaction Calculator Rationale

https://coi.avpreserve.com/rationale

This is a great information video from AVPreserv on the cost of inaction and the business case rationale for digital preservation. It is focussed on Audio-Visual material but it worth listening to and thinking laterally about the underlying rationale whatever type of digital material you hold. (8mins 41sec)

Case studies

KRDS Benefits Toolkit case studies

There are 4 case studies providing worked examples of completed worksheets from project partners as follows:

Archaeology

http://www.ukoln.ac.uk/events/i2s2-krds/presentations/catherine-hardiman-krds-benefit-framework-2011-07-v2.ppt

The background to this case study is provided in the Archaeology Data Service (ADS) dissemination workshop presentation. Worked examples are available of the ADS Benefits Framework Worksheet (PDF) and the ADS Value-chain and Impact Worksheet (Excel 97-2003).

Health: Population Cohort Studies

http://www.ukoln.ac.uk/events/i2s2-krds/presentations/dipak-kalra-krds-benefits-2011-07.ppt

The background to this case study is provided in the Medical Research Council Cohort Studies dissemination workshop presentation. A worked example is available of the Cohort Studies Value-chain and Impact Worksheet (Excel 97-2003).

Research Data Citation: SageCite

http://www.ukoln.ac.uk/events/i2s2-krds/presentations/monica-duke-krds-sagecite-benefits-2011-07.ppt

The background to this case study is provided in the SageCite dissemination workshop presentation. A worked example is available of the SageCite Benefits Framework Worksheet (PDF).

Social Sciences: UK Data Archive (UKDA)

http://www.ukoln.ac.uk/events/i2s2-krds/presentations/matthew-woollard-krds-benefits-2011-07.ppt

The background to this case study is provided in the UKDA dissemination workshop presentation. A worked example is available of the UKDA Benefits Impact Worksheet (PDF).

Digital Preservation Business Case Toolkit

There are four case studies as follows sourced from activities conducted as part of SPRUCE Project Awards:

Bishopsgate library case study

http://wiki.dpconline.org/index.php?title=Bishopsgate_library_case_study

A collections audit and business case focused on taking the first steps of digital preservation.

Institute of education case study

http://wiki.dpconline.org/index.php?title=Institute_of_education_case_study

A review of approach and generation of a business case for digital administrative record keeping.

Northumberland estates case study

http://wiki.dpconline.org/index.php?title=Northumberland_estates_case_study

Assessment of digital repository solutions and an associated business case for digital preservation.

Lovebytes case study

http://wiki.dpconline.org/index.php?title=Lovebytes_case_study

A trial of media stabilisation and content preservation along with a business case to move to a production status.

References

Keeping Research Data Safe (KRDS), 2011. *Digital Preservation Benefits Analysis Toolkit*. Available: http://beagrie.com/krds-i2s2.php