




Catalogue of preservation policy elements

Authors

Barbara Sierman (Royal Library of the Netherlands), Catherine Jones (Science and Technology Facilities Council), Gry Elstrøm (State Library of Denmark)

February 2014

This work was partially supported by the SCAPE Project. The SCAPE project is co-funded by the European Union under FP7 ICT-2009.4.1 (Grant Agreement number 270137).

This work is licensed under a CC-BY-SA International License 

Catalogue of Policy Elements



Executive Summary

This Catalogue of Policy elements is part of the policy framework in SCAPE. The SCAPE policy framework is based on one of the aims in the SCAPE project: that the preservation functions Planning and Watch will make use of automated policy compliant workflows. Automated policy compliant workflows will need detailed preservation policies that are directly derived from higher level –less detailed formulated – policies. This is reflected in the SCAPE Policy Framework.

The framework consists of three preservation policy levels going from a high level abstract view of preservation within an organization, the Guidance Policy, to more defined descriptions of policy intent, the Preservation Procedure Policies, through to concrete applicable statements which can support automated workflow, the Control Policies. This Catalogue of Policy elements will describe the middle level, the Preservation Procedure Policies, in more detail and with references to the other levels. By connecting these three levels the aim is to make the creation of a preservation policy for organisations more straightforward, to raise the awareness of the need for more detailed formulated policies and to enable them to be better prepared for machine readable policies.

Table of Contents

.....	i
Catalogue of Policy Elements	iii
Deliverable	i
Executive Summary	iii
1. Introduction to the Catalogue of Policy Elements	1
1.1. Scope of the Catalogue of Policy Elements	2
1.2. Why this Catalogue of Policy Elements?	2
1.3. Approach chosen to create this Catalogue of Policy Elements	3
1.4. Preservation Policies and different types of objects	4
1.5. Adaptation of the Framework of Preservation Policies	4
2. Policies in other European projects	4
2.1. Shaman : Sustaining Heritage Access through Multivalent Archiving	4
2.2. Planets	5
2.3. DL.org	5
2.4. Current EU projects	6
3. The SCAPE Framework of Policies	7
3.1. Guidance Policy Identification	8
3.2. Preservation Procedure Policies	8
3.3. Control Policies	8
3.3.1. Process flow	9
3.4. Conclusions	12
4. The description of the catalogue of policy elements	14
4.1. The policy element template	14
4.2. DCC Life cycle model	15
4.3. Stakeholder	17
5. Guidance policy: Authenticity	19
5.1. Preservation Procedure Policy: Integrity	20
5.2. Preservation Procedure Policy: Reliability	22
5.3. Preservation Procedure Policy: Provenance	23

6.	Guidance Policy: Bit Preservation	25
6.1.	Preservation Procedure Policy: Define Bit preservation	26
6.2.	Preservation Procedure Policy: Define Bit preservation levels	27
6.3.	Preservation Procedure Policy: Decide on Ingest activities	29
6.4.	Preservation Procedure Policy: Develop Integrity Measures	31
6.5.	Preservation Procedure Policy: Persistent Identifiers	32
6.6.	Preservation Procedure Policy: Decide on number of copies, geographical distribution and organisational distribution	34
6.7.	Preservation Procedure Policy: Defining Policy for Disaster Recovery	36
7.	Guidance policy: Functional Preservation	38
7.1.	Preservation Procedure Policy: Plan functional preservation	39
7.2.	Preservation Procedure Policy: Define preservation strategies	41
7.3.	Preservation Procedure Policy: Define Ingest activities / preservation actions	44
7.4.	Preservation Procedure Policy: Keep track of versions when performing migration	45
8.	Guidance Policy: Digital Object	47
8.1.	Preservation Procedure Policy: Original object	48
8.2.	Preservation Procedure Policy: Deletion of objects	49
8.3.	Preservation Procedure Policy: Keep track of developments of file formats	50
8.4.	Preservation Procedure Policy: Take-down policy	52
8.5.	Preservation Procedure Policy: Define significant properties	54
9.	Guidance policy: Metadata	56
9.1.	Preservation Procedure Policy: Metadata: Management of metadata	57
9.2.	Preservation Procedure Policy: Metadata: Original metadata	59
9.3.	Preservation Procedure Policy: Metadata: Descriptive metadata	61
9.4.	Preservation Procedure Policy: Metadata: Preservation metadata	63
9.5.	Preservation Procedure Policy: Metadata: Structural metadata	65
10.	Guidance Policy: Rights	66
10.1.	Preservation Procedure Policy: Comply with national legislation and contracts with business partners	67
10.2.	Preservation Procedure Policy: Document Object creator /copyright holder	69
10.3.	Preservation Procedure Policy: Enter into deposit and archiving agreements	70

10.4. Preservation Procedure Policy: Clarify legal context for preservation actions	72
11. Guidance Policy: Standards	74
11.1. Preservation Procedure Policy: Principle on the use of standards	75
11.2. Preservation Procedure Policy: Reference Model	77
11.3. Preservation Procedure Policy: Use of specific standards	79
12. Guidance policy: Access	81
12.1. Preservation Procedure Policy: Usability	82
12.2. Preservation Procedure Policy: Digital Rights Management (DRM)	84
12.3. Preservation Procedure Policy: Design of Dissemination Information Package	86
12.4. Preservation Procedure Policy: Understandable for Designated Community	88
12.5. Preservation Procedure Policy: Search facilities / resource discovery	90
12.6. Preservation Procedure Policy: Designated Community/Communities identified	91
13. Guidance Policy: Organisation	93
13.1. Preservation Procedure Policy: Staffing	94
13.2. Preservation Procedure Policy: Risk Management	96
13.3. Preservation Procedure Policy: Budgets	97
13.4. Preservation Procedure Policy: Preservation Cost Assessment	98
13.5. Preservation Procedure Policy: Roles and Responsibilities	99
14. Guidance policy: Audit and Certification	101
14.1. Preservation Procedure Policy: Standard for Audit and certification	102
14.2. Preservation Procedure Policy: Audit preparations	104
15. Further Reading	105

1. Introduction to the Catalogue of Policy Elements

This Catalogue of Policy elements is part of the policy framework in SCAPE. The SCAPE policy framework is based on one of the aims in the SCAPE project: that the preservation functions Planning and Watch will make use of automated policy compliant workflows. The framework consists of three preservation policy levels going from a high level abstract view of preservation within an organisation to more defined description of policy intent through to concrete applicable statements which can support automated workflow. By connecting these three levels we intend to make the creation of a preservation policy for organisations more straightforward and enable them to be better prepared for machine readable policies. This framework is described and discussed in Chapter 3.

In this document the word “organisations” will be used for organisations that “owns” or keeps running a repository in which digital material is preserved for the long term and “users” will be used for the users of the digital collections, including the Designated Community, “Consumers” and internal users.

In order to make the automated policy compliant workflows applicable for individual organisations, their organizational policies need to be incorporated. Therefore the policies within workflows need to be at a detailed level. But for other purposes like communication with their funding agencies, producers & deliverers of the digital material and the consumers and other colleagues within the organisation organisations will need policies on a higher, more abstract, level.

The Catalogue of Policy Elements gives an overview of the essential policy elements that an organisation will need to formulate in order to be able to derive the level of policies needed to run policy compliant workflows. The Catalogue of Policy Elements also offers organizations an opportunity to create their own set of policies, by explaining various aspects of each policy element. The current set of policy elements however, will be subject of changes and additions. Digital preservation is a relatively new topic and the insights on “how to do” digital preservation will change as the approaches will get more mature. Developments in various areas like different types of objects to preserve, different responsibilities in who will preserve what and a growing maturity in the approaches to choose from, will lead to extensions and perhaps deletions in the current set of policy elements.

When looking at existing, published policies of organisations (as part of the activities of this work an overview was given at the OPF website), we see quite often that the policies are formulated on a very high level, reflecting the ambitions of the organisation with the preserved digital collections. This high level of policies however, will often be not sufficient to create automated policy compliant workflows, as will be explained in chapter 3. On the other hand, it might well be possible that organizations also formulated more detailed policies to guide their preservation activities, but decided not to publish them, and so they were not part of our investigation.

Compared to the number of organisations that have a preservation mandate, only a few of them have made their preservation policy publicly available. The Open Archival Information System (OAIS) model, which is for many organizations with a digital collection a starting point, requires that the organization follows documented policies and procedures (see Mandatory responsibilities OAIS 2012) although it does not say that they need to be publicly available. The ISO 16363 Standard for Audit and Certification emphasizes in various metrics the importance of having formulated preservation policies in order to be able to realise the preservation strategic plan and sees policies as essential element.

Policies are important and essential to have. They will help to raise awareness and guide various parts of the organisational staff in their activities related to digital preservation. They will be an useful instrument in the everyday work of preservation professionals. They will support decision making, help to choose the right preservation actions and will support the quality assurance of these actions. The users and the producers of the preserved collections will benefit if they can read the preservation policies, as they will give them an overview of what to expect from an organisation (what will be preserved, for how long, how it will be accessible etc.). Needless to say that also colleagues in digital preservation can benefit from reading the preservation policies of other organisations.

1.1. Scope of the Catalogue of Policy Elements

This Catalogue of Policy Elements is restricted to what is called “Preservation Policies” and in the SCAPE project defined as

“Preservation policies should provide the mechanisms to document and communicate key aspects of relevance, in particular drivers and constraints and the goals and objectives motivated by them. They are to support the activities of an organisation with respect to the maintenance and preservation of a digital collection.” [SCAPE Glossary](#).

But preservation policies cannot be seen in isolation from other policies. Therefore in Preservation Policy and organisation will often refer to other relevant policies in the organisation, like for example Collection Policies, Harvest Policies in case of web archiving and Data Acceptance policies for research data etc.

1.2. Why this Catalogue of Policy Elements?

The SCAPE project is dedicated to the challenges of large scale, heterogeneous collections of complex digital objects. The digital objects are held in the collections of various participating content holders, like libraries, web archives and data centres. The scale of these digital collections implies that preservation activities that need to be performed will limit the possibility of manual involvement, and require more automation through the use of workflows and high-performance systems. The automated workflows performing the preservation activities will need to be based on the organizations preservation policy.

In digital preservation, a preservation action will often be preceded by an identified risk, based on monitoring several areas of interest, and a combination of the outcomes leading to a decision to act. The identification of the most appropriate action is done in the Preservation Planning process, which produces a preservation plan. Enacting the preservation plan will result in the Preservation Action. In SCAPE the Preservation Watch area will be enriched by the SCOUT system. SCOUT is an automatic preservation watch system that is designed to detect preservation risks and opportunities. The Preservation Planning will be extended by new versions of the Preservation Planning tool PLATO2. In both cases, a detailed level of preservation policies will be needed to enable the planning and watch services to act according to a specific set of institutional preservation policies.

The Catalogue of Policy Elements is built upon ideas developed in the Planets Project, especially the Planets Functional Model. Here Preservation Watch uses the information of the organisational preservation policies to formulate risks and constraints for the Preservation Planning activity. On the other hand, preservation policies can be updated as a result of

Preservation Planning and action activities and other changes in the environment of the organisation, monitored by Preservation Watch. Another dependency exists between organisational policies and policy-aware characterisation tools.

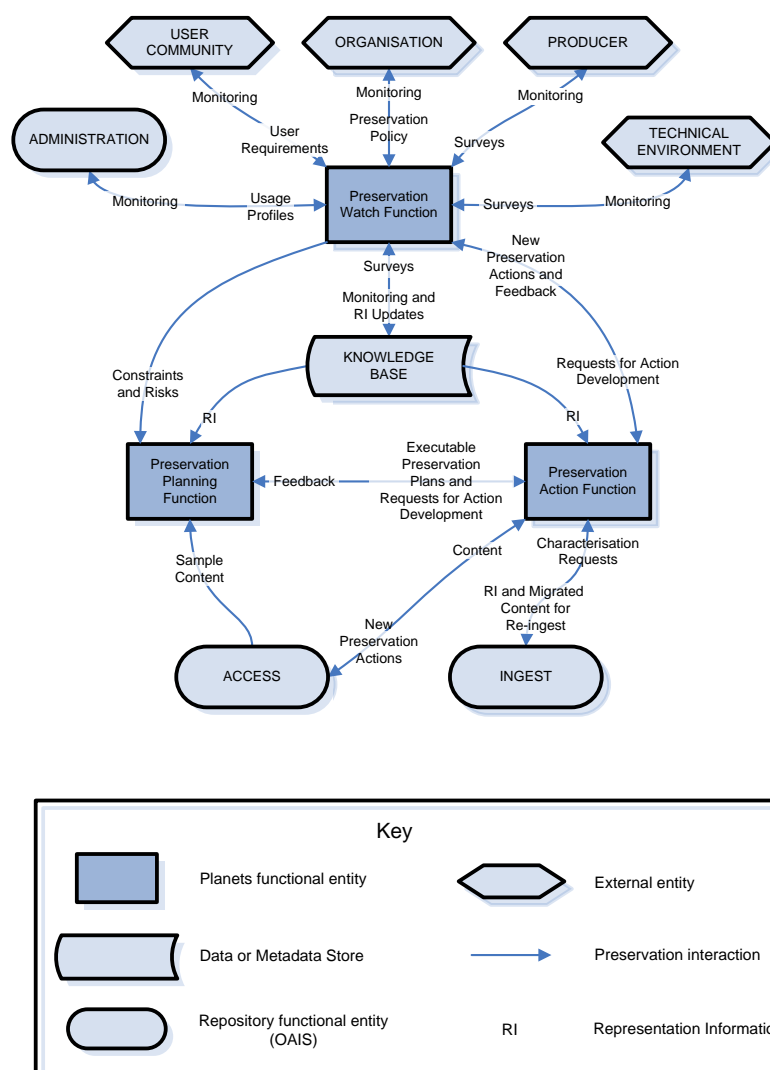


Figure 1 Planets Functional Model

1.3. Approach chosen to create this Catalogue of Policy Elements

The approach taken to create the Catalogue of Policy Elements has undertaken the following steps:

- Desk top research and collecting relevant standards and guidance in relation to preservation policies. This included the OAIS standard, the Beagrie report Digital Preservation Policy Study, the standards related to Audit and Certification (TRAC, DSA, ISO 16363), see Further Reading. Based on these findings a set of main policies were distilled, which were input for the development of the Framework.
- Development of the SCAPE Framework of Policy Levels, described in chapter 3
- Discussing and publishing via blogposts and articles the Framework with preservation professionals on various occasions like iPRES 2013, SCAPE training events in Glasgow and

Aarhus, presentations on meetings of the IIPC and Florence and in the SCAPE project internally.

- Examining the policy related activities in currently running other European projects, with a reference to policy work in their plans. The results of this are summarized in chapter 2
- Collecting relevant policy elements and mapped them to the various levels
- Developing and completing a template for the Catalogue of Policy Elements
- Comparing the findings with a set of published policies we collected, with input from the publication of [M. Sheldon in The Signal](#). The results of the collected policies were [published](#) on a wiki, and we encouraged people via blogs etc. to add their preservation policy to the collection. For this work we used the collection to check whether the Catalogue was complete.

1.4. Preservation Policies and different types of objects

In the SCAPE project the focus is on three different types of data collections: web archives, (large scale digital) repositories and research data. But does this also mean that each type of repository will have a different Catalogue of Policy elements? One of the conclusions we drew, based on looking at the set of published policies, was that this depends on the level of the preservation policy. On the main level, the policies did not make a distinction in various types of objects. There are policies for data collections, but they don't necessary differ from the ones for large repositories with publications. For web archiving there were hardly any examples to find. So on the main level it seems that the policies can be similar for various types of collections.

The lowest level of policies however, used to guide the preservation actions; the distinction to various types of objects will be more relevant. The work related to Preservation Watch, Preservation Planning and the Control Policy Model in SCAPE will discuss this more in detail (chapter 3).

This Catalogue of Policy Elements should be applicable for all three types that are in focus of the SCAPE project.

1.5. Adaptation of the Framework of Preservation Policies

The Catalogue of Policy Elements is part of the Framework of Preservation Policies. This Framework will consist of 3 – interrelated - levels of Policies, the Catalogue describing the elements of the intermediate level. In order to be useful on the level of policy driven preservation actions, the lowest level need to be described and more detailed information will be needed. During the SCAPE project a start for such detailed policies has been made and will be described in chapter 3. It would be beneficial for organizations if also these detailed policies would be published and shared within the community.

2. Policies in other European projects

2.1. Shaman: Sustaining Heritage Access through Multivalent Archiving

Reference Architecture, 2011 [SHAMAN-REFERENCE ARCHITECTURE-Final Version.pdf](#)

The SHAMAN report, 2011, has a holistic approach to system architecture and digital preservation. The report analyses primarily business perspectives in digital preservation and creates a vision for a reference architecture for digital preservation. In the report policies are defined as: “**Policies:**

Describe goals, constraints and strategies that are defined by the Governance Capabilities. The policies are essentially the instrument by which Governance Capabilities control Preservation Planning.” The SHAMAN Reference Architecture is written from a more technical development point of view than is used in this Catalogue of Policy Elements but the report has useful input on roles/stakeholders in digital preservation. The stakeholder definitions relevant for this Catalogue of Policy Elements are listed below in Chapter 4.3 Stakeholder.

2.2. Planets

Planets Functional Model – 2009 takes a more high-level view of preservation with 3 key components: preservation watch; preservation planning and preservation action and identifies 4 external entities

- User community
- Organisation
- Producer
- Technical Environment

Report on the Conceptual Aspects of Preservation, Based on Policy and Strategy Models for Libraries, Archives and Data Centres, 2009

- Aimed to produce a conceptual model for supporting preservation policy and strategy within an organisation
- Defines preservation policy as “[PP2 based on InterPARES23] *A formal statement of direction or guidance as to how an organization will carry out its preservation mandate, functions or activities, motivated by determined interests or programs.*”
- Policy & strategy represented by a concept called PreservationGuidingRequirementsSet. Refines & extends the notion of “organisational policy and strategy”

Report on Policy and Strategy Models for Libraries, Archives and Data Centres, 2008

- *“There is no consistent distinction drawn between what constitutes a preservation ‘policy’ versus a ‘strategy’. The terms are used variously and the delineation between them varies in different institutions. We have introduced a more general term, preserving guiding documents, to cover policies, strategies, and a variety of other documents that give guidance to preservation planning and other key preservation processes.”*
- No high level elements were proposed; rather the focus of the work was on the conceptual model rather than the content of the model.

These PLANETS documents point the way towards the work done in SCAPE as it identified a gap which this work in SCAPE addressed.

2.3. DL.org

A digital library in the DL.org project is a name applicable for a wide variety of organisations with digital collections, as it is characterized in their [Digital Library Technology and Methodology Cookbook](#) as *“the infrastructure, policies and procedures, and organisational, political and economic mechanisms necessary to enable access to and preservation of digital content”* (p. 5) It is seen as crucial here that every digital library has formulated a framework of policies as “without a policy framework a digital library is little more than a container for content.” The DL.org project focuses on policies as part of interoperability between digital libraries and emphasizes the fact that policies “governs how a digital library is instantiated and run”. With regard to (preservation) policies, the advice is to make use of standards. A description of a set of relevant standards for preservation policies is given on page 69 of the Cookbook preservation policies. A brief reference is made to the

benefit of making policies machine readable, as it will make them easier to manage (p. 68) while also briefly mentioning “Policy-based data management which captures policies as computer actionable rules.”(p. 123). This element however is not further worked out in the project.

2.4. Current EU projects

Based on a literature search at two moment during the project (2012, 2013) during the projects, we can conclude that current EU projects discussed below have not had a particular focus on policy in general or preservation policy in particular. Where they have addressed policy it has focussed on the rights to collect and preserve material.

APARSEN is a Network of Excellence focused on bringing coherence, cohesion and continuity to research into barriers to the long-term accessibility and usability of digital information and data. There is a current work on Data Policies and Governance which has not yet reported and so it is not incorporated into this work.

ARCOMEN Research project on identifying and preserving relevant social media content.

BLOGFOREVER: examined preservation of blogs. D3.3 Development of the Digital Rights Management Policy discussed specifics of policies for organisations which harvest blogs.

PRESTOPRIME: research and develop practical solutions for the long-term preservation of digital media objects, programmes and collections. There are some recommendations on digital rights.

WF4EVER: the project addresses the preservation of scientific workflows in data intensive science. Preservation driven by user interactions so organizational preservation policy not addressed.

3. The SCAPE Framework of Policies

The SCAPE Preservation Policy Framework consists of three preservation policy levels that can support an organisation in creating their preservation policies set. By connecting these three levels and identifying clearly which level is fit for which purpose, we intend to make the creation of a preservation policy for organisations more straightforward and better prepared for machine readable policies.

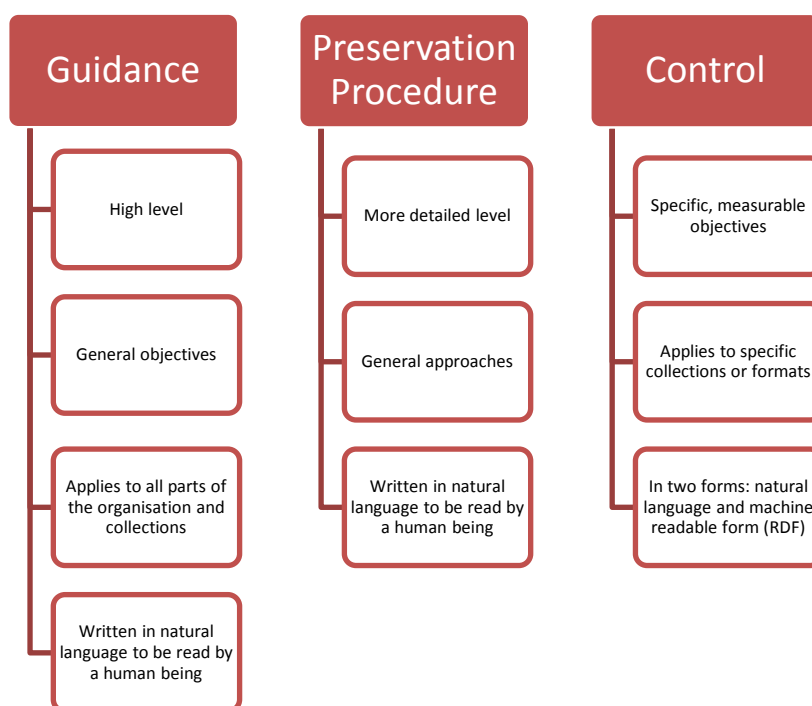


Figure 2: The three levels of preservation policy identified in SCAPE

Guidance policies. On this level the organisation describes the general long term preservation goals of the organisation for its digital collection(s). One example is that an organisation decides that the infrastructure in place to provide digital preservation will be guided by the OAIS model.

Preservation Procedure level policies: These policies describe the approach the organisation will take in order to achieve the goals as stated on the higher level. They will be detailed enough to be input for processes and workflow design but can or will be at the same time concerned with the collection in general.. This is the level that is the topic of the Catalogue of Policy Elements.

Control Policies: On this level the policies formulate the requirements for a specific collection, a specific preservation action or for a specific designated community This level can be human readable, but should also be available in machine readable and actionable form and thus can be used in automated planning and watch tools to ensure that preservation actions and workflows chosen meet the specific requirements identified for that digital collection.

What information about policies is made public depends on the remit of the organisation. We would suggest that the guidance policies should be available to the user community; whereas the control policies are too detailed and may have operational information which should be kept internally. How available the preservation procedure level policies are depends on the organisation and their user community.

3.1. Guidance Policy Identification

Based on a literature research (see Further Reading) key policy areas were identified. The intention was to identify the areas that comprehensive policy should cover and was likely to translate into preservation procedure and control policy levels. The list below summarises the initial starting point.

- Authenticity, measures to establish authenticity
- Preservation Goals, which goals does an organization want to achieve
- Preservation Strategies, ways of achieving the goals
- Metadata, policies related to metadata
- Organisation, policies related to the behaviour and tasks of the archival organization
- Standards, the applicability of standards
- Designated Community, policies related to the users of the digital archive
- Storage, policies related to the storage of digital objects
- Formats, policies related to file formats
- Rights, policies related to access, preservation, IP etc. rights
- Trustworthy Digital Repositories, policies related to the aim to become a TDR.

The initial list was reviewed and the topic of digital object was added. The digital object was not an explicit area in the literature, but underpins all policy making. The topic of “Preservation Goals” was removed as although it is a very important concept for the organisation to decide, the practical activities in meeting the preservation goal are covered in the other key areas. Trustworthy Digital Repositories was also identified specifically in the literature and although it could be treated in the same way as preservation goals, it was decided that there were some specific preservation procedure policies relating to the undertaking of an audit and so it was kept.

The final set of key policy areas used in the Catalogue of Policy Elements is as below:

- Authenticity
- Bit Preservation
- Functional Preservation
- Digital Object
- Metadata
- Access
- Rights
- Standards
- Organisation
- Audit and Certification

These final ten areas underpin the work on the preservation procedure level elements and form the basis for the work in this deliverable.

3.2. Preservation Procedure Policies

This document is, amongst others, concerned with the creation of Preservation Procedure policies and is not further discussed in this section.

3.3. Control Policies

To be able to produce the machine readable based on the natural language original there needs to be a translation process and this section describes such a process. The control policy model was described in full in D13.1. It links particular objectives, to content sets and user communities using a particular preservation case. The objectives should be such that the outcome can be quantified: for example that the file format must be a JPEG. These control policies are defined as practicable elements of governance that relate to clearly identified entities in a specified domain model.

The policy model provides vocabulary that is used to describe particular domain entities: situations, formats, content sets etc. Key entities described in the model are as follows:

- **Content Set.** A Content Set represents a collection of objects that are the focus of the policy
- **User Community.** The community for whom digital content is preserved for.
- **Preservation Case.** A Preservation Case ties objectives to a Content Set and intended User Community
- **Objective.** Objectives are the atomic building blocks of the policies. Objectives may refer to properties that representations of content have; properties of the formats themselves; tools used and so on. Objectives are defined in terms of measures which are taken from a catalogue.

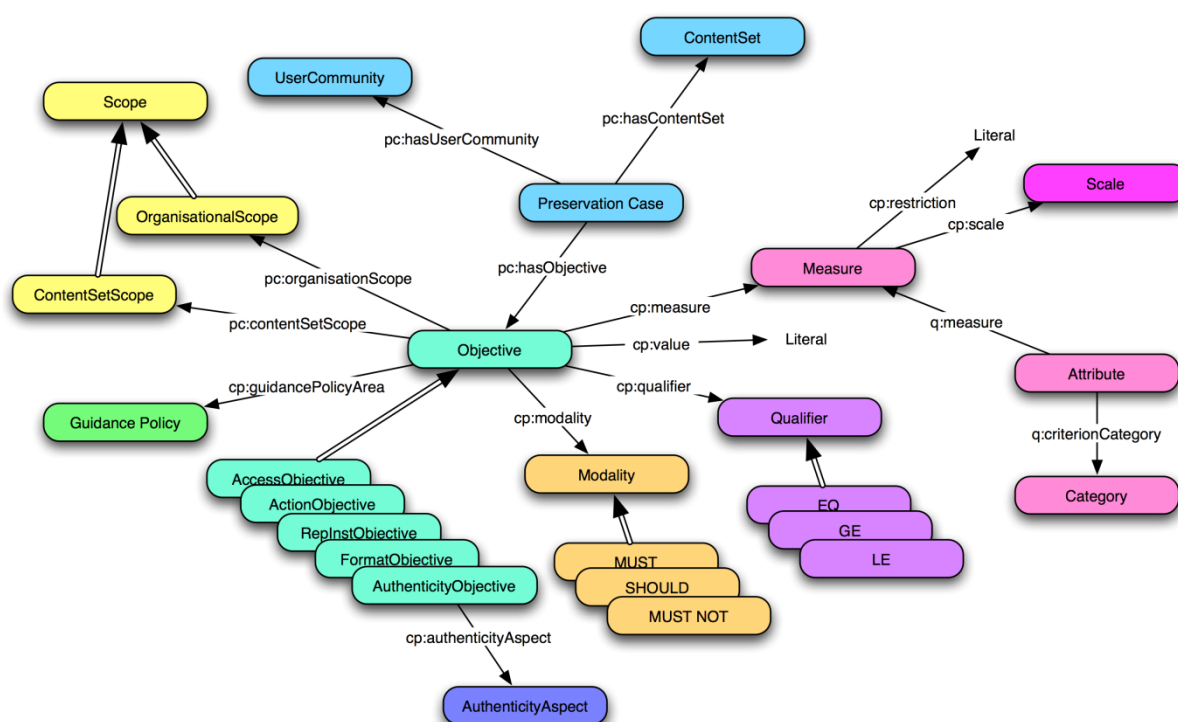


Figure 3 Overview of the SCAPE Control Policy Model

Translating human readable policy into machine readable policy takes a substantial amount of human effort, so it is likely in practice to be limited to the areas where machine readable policy will create the most benefit to the organisation. Within the SCAPE project, the two areas where machine readable policy is being used to support automation is in watch, through the use of SCOUT, and planning, through the use of PLATO, so although this translation process is applicable to all areas of policy, our examples have concentrated on areas which might be used in planning and watch.

3.3.1. Process flow

The chart below shows the steps needed to get from written policy to control level policy. To be able to undertake the translation, the written natural language policy must be available.

There are three stages – the first applies to the preservation procedure policy/human readable control policy as a whole, the second stage to the policy fragments within a larger policy and the final stage is a review of the results.

Stage 1: Whole policy activities

Stage 1.1: Identify the content set that the policy addresses

Define or identify the content set the policy is being applied to, and consider whether this will be the same for the control policy level



Stage 1.2: Identify the user communities/roles required by the policy

Identify the different roles addressed in the policy

Stage 1.1: Identify the content set which is addressed by the policy

The content set is an intellectually cohesive collection of digital objects to which all the objectives within a preservation case apply. Some consideration as to the make-up of the content set needs to be made to ensure there are no exceptions within the content set. So the content set for control policies may not exactly overlap with the collection being described in the preservation procedure document due to the shift in emphasis & use between natural language policy and machine readable policy.

To enable the use of organisational objectives, a content set can be part of a larger content set.

Stage 1.2: Identify the user communities/roles required by the policy

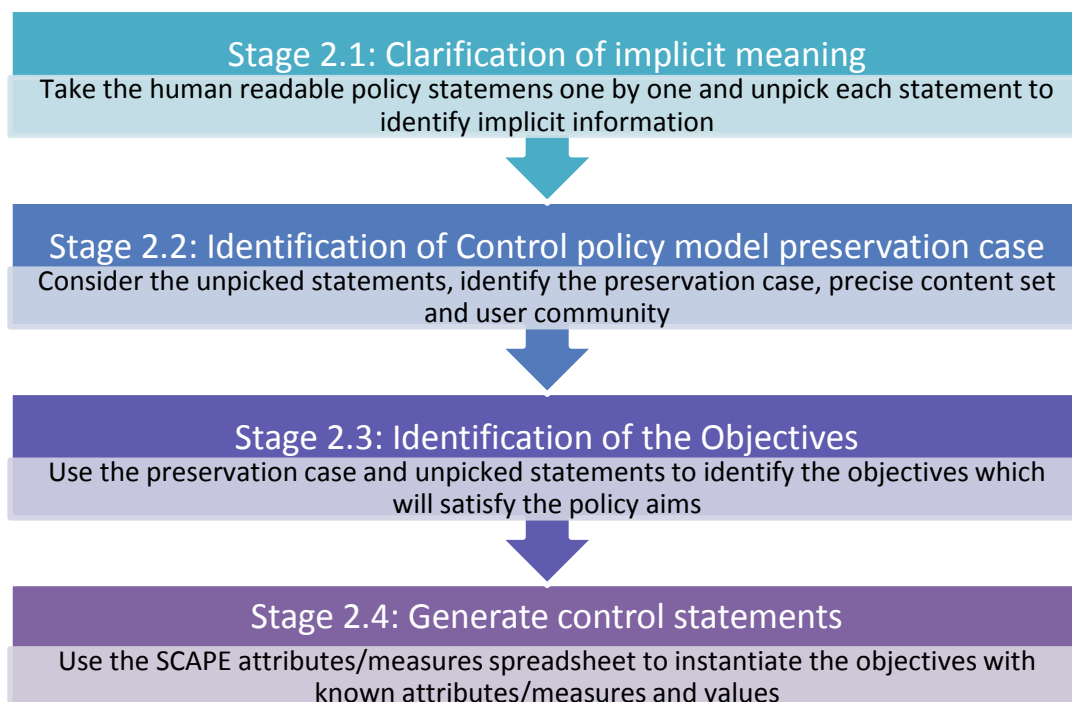
The identification of the user community(ies) is an important facet of the control policy model development as it defines the group of people who have a specific role/use case within the preservation scenario.

At a minimum there will be the curators/managers of the collection/digital objects and the potential users of the preserved digital objects, as these two roles are fairly universal. The third obvious role is that of the data creator/original owner, but once the data is ingested within the system, there may be less of a direct role in control level policy. For collections/content set which have special restrictions, there may be distinctions in one or both of these basic underpinning roles.

As a starting point, we recommend that fine distinctions are made, as it is easier to merge categories at the end than it is to make finer grained distinctions at the end of a process. It should, however, be possible to identify these user communities uniquely electronically in some way.

Stage 2: Policy statements within the whole policy activities

For each of the relevant lines in the human readable policy, follow the procedure below:



Stage 2.1: Clarification of implicit meaning

Natural language policy is written by humans in a specific context (organisation, legal framework, etc.) and it is usually intended to be used and read by others who are based in the same context, therefore there may be information that machine actionable statements would need to know which are not explicitly stated in the written document. To be able to create concrete unambiguous control policies it is important to ensure that the natural language originals are represented in an unambiguous way. Whilst it is the aim for policy makers to be precise when making policy, it is not possible using natural language to be completely unambiguous, especially to those outside the organizational context.

This stage is designed to check for and remove as much implicit contextual meaning within the natural language version being worked on so that the resulting control policy statements are as unambiguous as possible. This is not a straight-forward activity as part of the issue of implicit information is that one doesn't realize that, if one knows the context, that a human will add personal knowledge to the written language to full comprehend the meaning. A couple of examples of this are

- Using the term “*curated*” in a policy document: what in practice does this actually mean, what activities does this entail? Does the term curated refer to further documentation where it is further defined?
- In an organisation where a document management system, such as Sharepoint, is used then there would be a common understanding of the fact that documentation is centrally kept and automatically versioned and might not be explicitly mentioned in policy.

Stage 2.2: Identification of control policy preservation case

Having unpicked the natural language policy, the next step for each element/policy statement is to decide on the user communities who have an interest in this, what the content set is in question and using the high level term decided on stage 1.3, to make an initial choice of the preservation case contained within this policy fragment.

The control policy model preservation cases enable the link between a content set, a specific user community and the objectives required satisfy this combination to be made. The final preservation

cases are likely to emerge at the end of the process once the entire natural language policy has been through the process.

Stage 2.3: Identification of objectives

Using the content of the policy statement, identify the testable objectives which a machine could use to ensure the intent behind the natural language statement. Keep in mind whether these objectives only apply to this particular combination of user community and content set or might apply for other combinations of user community and content set.

Stage 2.4: Generate control policy statements

Either using a tool, or creating RDF by hand, transfer the objectives into RDF statements with specific measurable statements.

The SCAPE control policy implementation used an internal measure and attributes controlled list to enable the objectives to be realised.

Stage 3: Review the Preservation Cases and identify any rationalisation required

Stage 3.1: Review the preservation cases identified

Review the results of the conversion from policy fragments to look for overlap and duplication. Ensure that the preservation cases have different sets of objectives, duplicate sets are candidates for organisational level control policy set

Stage 3.1 Review the preservation cases identified

After the completion of Stage 2, a check should be made to ensure that the preservation cases are distinct and if there is significant overlap then combining preservation cases or adding them to organisational level control statement sets should be considered.

3.4. Conclusions

It is important to consider the three different levels and audiences of policy required to underpin both human and automated actions and this project aimed to assist in the creation of more formal explicit policy to assist those with responsibilities in this area.

Guidance and Preservation procedure policies are concerned about the allowable and not allowable states and don't necessarily address actions/activities. These are likely to be currently done in collection specific policies, implementation plans/task related procedures or special one-off project plans. This means that control policies for some types of preservation activities are unlikely to be generated through consideration/translation of policy documents.

Going forward there is the possibility that standard sets of control policies could be generated which could be modified by particular organisations. For example sets of control policies based on types of digital object and user community. This would aid adoption of the control policy model and would also assist in common usage and practice within the community.

Generating control policies at the moment requires a lot of manual intervention and a future development to enable validation of the control policies generated would be to implement a process to derive preservation procedure policies from control policy statements so that the organisation can be confident that the control policies generated do in fact implement the preservation procedure policy(s) accurately. Currently the link between guidance/preservation procedure policies is done through ensuring specific linkages/relationships are made between control statements and the higher levels.

The Research Data Alliance has a working group on practical policy and will collect together results from various areas and different viewpoints. The work done in SCAPE is reported there and this collaboration will hopefully lead to further developments.

4. The description of the catalogue of policy elements

For the description of the policy elements a template was designed, each policy element is described by a standard set of characteristics. Together the characteristics should give the reader enough information about why and when the policy element is important. This chapter will explain the various boxes in the template. In addition to the elements, chapter 15 contains “Further Reading.” Although this report does not offer a complete set of relevant literature, for some policy elements, like for example authenticity, literature exists that might support the organisation further in defining their policy.

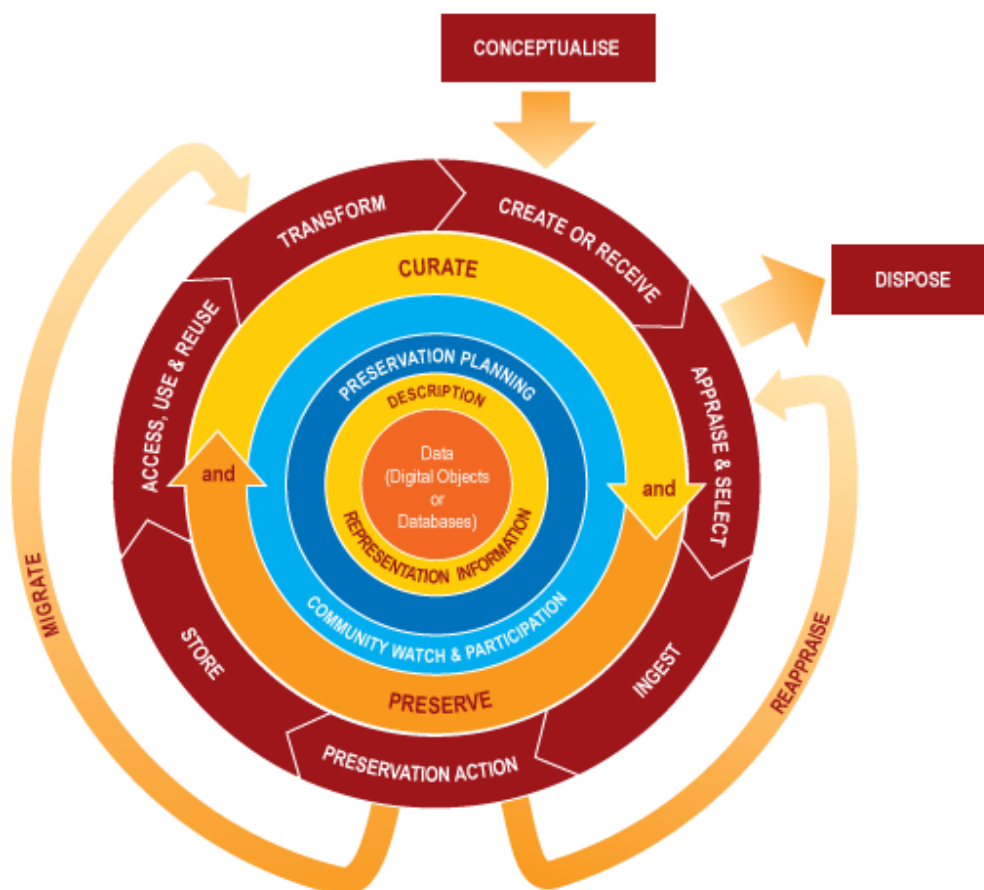
4.1. The policy element template

Preservation Procedure Policy: Name of the policy element	
Related Guidance Policy	Because every policy element should be readable independently, the related higher level, the Guidance Policy, is mentioned.
Definition/Description	Every policy element will have a description and, if applicable, a definition, based on existing glossaries in standards like the OAIS model or digital preservation glossaries, such as the APARSEN project or the InterPARES project . The source of the definition will be referenced.
Why	An explanation is given why it is important that an organization defines a policy related to this element.
Risks	Not having a written policy could imply various risks for the organization and in this box some examples will be given. Of course whether the risk will occur is dependent on several factors; the examples are added to stimulate further discussions. Apart from general knowledge, also standard literature like DRAMBORA and ISO 16363 can be used in these internal discussions.
Life cycle stage	The intention of this box is to put the policy element in relation to the life cycle stages it might be relevant for and to achieve a coherence in policy elements for different life cycles. As the basis the DCC life cycle model is used (see 4.2).
Stakeholder	It is important that someone in the organisation will be responsible for describing the preservation policy, in relation to the processes the policy relate to and in coherence with the other processes in the organisation. This person is called a “stakeholder”. The SHAMAN project distinguished a set of stakeholders in relation to digital preservation and these are used where applicable (see 4.3).
Cross Reference	It is seldom that a policy element stands in isolation. More often a policy element is related to other policy elements, where applicable this relationship is mentioned.
Examples	To illustrate the policy element, one or more relevant examples of Preservation Policies were taken, based on the collected policies . This could be used as an inspiration for organisations to create their own version.

Control Policy	As mentioned before, we have related the control policies to two cases: Preservation Watch and Preservation Planning, as these are the areas in the SCAPE project where the control policies will be used.
Questions to foster discussions	If an organization wants to create preservation policies, it will be important to engage different people in the organization (the “stakeholders”) and together phrase the relevant policies. The set of questions for each element will help starting the discussions and highlight the various aspects of the policy element, like the risk of not having thought of the policy element.

4.2. DCC Life cycle model

For readers convenience the description of the life cycle stages of the [DCC Curation Life Cycle Model](#) of the Digital Curation Centre is cited here. In many cases the “full life cycle actions” were applicable, like Curate and Preserve. Some more detailed policy elements however were related to a more detailed level, in the DCC model referred to as “sequential actions” or “occasional actions.”



FULL LIFECYCLE ACTIONS

1. Description and Representation Information

Assign administrative, descriptive, technical, structural and preservation metadata, using appropriate standards, to ensure adequate description and control over the long-term. Collect and assign representation information required to understand and render both the digital material and the associated metadata.

2. Preservation Planning

Plan for preservation throughout the curation lifecycle of digital material. This would include plans for management and administration of all curation lifecycle actions.

3. Community Watch and Participation

Maintain a watch on appropriate community activities, and participate in the development of shared standards, tools and suitable software.

4. Curate and Preserve

Be aware of, and undertake management and administrative actions planned to promote curation and preservation throughout the curation lifecycle.

SEQUENTIAL ACTIONS

5. Conceptualise

Conceive and plan the creation of data, including capture method and storage options.

6. Create or Receive

Create data including administrative, descriptive, structural and technical metadata. Preservation metadata may also be added at the time of creation.

Receive data, in accordance with documented collecting policies, from data creators, other archives, repositories or data centres, and if required assign appropriate metadata.

7. Appraise and Select

Evaluate data and select for long-term curation and preservation. Adhere to documented guidance, policies or legal requirements.

8. Ingest

Transfer data to an archive, repository, data centre or other custodian. Adhere to documented guidance, policies or legal requirements.

9. Preservation Action

Undertake actions to ensure long-term preservation and retention of the authoritative nature of data. Preservation actions should ensure that data remains authentic, reliable and usable while maintaining its integrity. Actions include data cleaning, validation, assigning preservation metadata, assigning representation information and ensuring acceptable data structures or file formats.

10. Store

Store the data in a secure manner adhering to relevant standards.

11. Access, Use and Reuse

Ensure that data is accessible to both designated users and re-users, on a day-to-day basis. This may be in the form of publicly available published information. Robust access controls and authentication procedures may be applicable.

12. Transform

Create new data from the original, for example: by migration into a different format, or by creating a subset, by selection or query, to create newly derived results, perhaps for publication

OCCASIONAL ACTIONS

13. Dispose

Dispose of data, which has not been selected for long-term curation and preservation in accordance with documented policies, guidance or legal requirements.

Typically data may be transferred to another archive, repository, data centre or other custodian. In some instances data is destroyed. The data's nature may, for legal reasons, necessitate secure destruction.

14. Reappraise

Return data which fails validation procedures for further appraisal and re-selection.

4.3. Stakeholder

It is important that someone in the organisation will be responsible for describing the preservation policy, in relation to the processes the policy relate to and in coherence with the other processes in the organisation. This person is called in the catalogue the “stakeholder”. The SHAMAN project distinguished a set of stakeholders in relation to digital preservation in their [Reference Architecture](#) version 3.0 and this was the basis for the catalogue. In one case the SHAMAN list did not offer a right description of the role intended, namely in the occasions where a stakeholder with a thorough knowledge of the collection was needed to phrase the policy element, so a role of Collection Manager (someone with a thorough knowledge of and responsible for the preserved collection), was added.

For convenience of the reader a summary of the SHAMAN stakeholders is added here.

1. **Producer/Depositor:** The entity responsible for the ingestion of the objects to be preserved. It may be the owner of the object, but it also can be any other entity entitled to perform this action.
2. **Consumer:** The entity representing the user accessing to the preserved objects, with a potential interest in its reuse and a certain background in terms of knowledge and technical environment.
3. **Management:** This entity is essentially a generalization of all management stakeholders, i.e. Executive Management, Information Manager, Technology Manager and Operational Manager
4. **Executive Management:** The entity responsible for strategic decision making on an organisation level, ensuring that the mandate is fulfilled. This entity defines strategic goals to be achieved by organization's systems and technology management.
5. **Information Manager:** The entity responsible for ensuring the organisation's systems business continuity, defining business strategies in line with strategic goals and setting goals and objectives to be achieved by operational management. That means it defines ends to be achieved by the organization, which have to be fulfilled by deployment and operation of means, but it also will define means on a strategic level.

6. **Technology Manager** The entity responsible for technological system continuity and the deployment of technological means to achieve the ends set by the preservation business. This entity effectively acts as a regulator to the operational manager, since the choice of technology limits the operational application of means to achieve ends.
7. **Operational Manager:** The entity that is responsible for continuous policy-compliant operation of the systems, which involves balancing ends and means and resolving conflicts between them, i.e. constraints as set from Technology Management and Preservation Management.
8. **Regulator** The entity responsible for external imposing rules concerning the preservation of digital assets, such as legislation and standards. Those can apply to the organisation, the system's technology, or the systems' usage
9. **Auditor** The entity responsible for the certification if the organization practices, the system's properties and the operational environments are complying with established standards, rules and regulations.
10. **Information Operator** The entity responsible for the preservation operations of the systems. This business worker may be aware of the details of the design and deployment of the system, but its mission is to assure the direct support to the business, with no concerns with the management of the infrastructure and no concerns about strategic alignment
11. **System Architect** The entity responsible for the design and update of the architecture of the system, aligned with the business objectives
12. **Solution Provider** The entity responsible for providing any kind of components of the architecture. This may include components, platforms and business services.
13. **Technology Operator** The entity responsible for the regular operation and maintenance of the components of the technical infrastructure (hardware and software) and their interoperability, according to specified service levels

5. Guidance policy: Authenticity

According to the [OAIS model](#) (page 1-9), authenticity is defined as: “The degree to which a person (or system) regards an object as what it is purported to be. Authenticity is judged on the basis of evidence.” The potential user of the collection in the repository, the Designated Community, will assess the authenticity of the digital objects and the repository owner will provide the evidence (idem, page 3-1). Therefore the repository owner or organisation needs to describe in policies which approaches will support the achievement of authenticity.

Organisations might approach the concept of “authenticity” from various angles, depending on their goals and character. So for example archives might do it differently compared to libraries, as they have different mandates.

According to [D24.1 Report on Authenticity and Plan for Interoperable Authenticity Evaluation System](#), written by the APARSEN project, the assessment can be done via technical and non-technical approaches. Technical approaches include using tools to validate the integrity of the bit sequences, fixity checks or provenance information. Non-technical approaches could include checking the identity of the producer of the digital object to be preserved. A combination of both approaches is usual.

Policy elements in this chapter

- 5.1 Integrity
- 5.2 Reliability
- 5.3 Provenance

5.1. Preservation Procedure Policy: Integrity	
Related Guidance Policy	Authenticity
Definition/Description	<p>Integrity checking covers approaches like encryption, digital signatures, fixity checks etc.</p> <p>See also the explanation in the section Bit preservation: Integrity measures</p>
Why	One of the main goals of digital preservation is that the preserved digital objects, once stored in the repository, are not changed without intent.
Risks	<p>If the organization does not explain the measures it will take to avoid unnoticed loss, it might not achieve its goals. The risks can occur in many stages of the digital life cycle. A digital archive needs to describe a set of approaches it intends to implement in order to avoid the risks. The measures to take are very related to the operational IT tasks and are often already part of their work, but the preservation policy needs to make explicit that these measures will contribute to the authenticity of the digital objects</p> <p>Relevant areas are:</p> <p style="padding-left: 40px;">Ingest: The completeness of the digital object will need to be defined before ingest and could be part of the discussion with the content deliverer or producer. At ingest the received checksums can be compared with the checksums generated upon retrieval. This will show whether bits were lost during transportation. This measure should be implemented for all data movements, including when the data is moved inside the repository.</p> <p style="padding-left: 40px;">Storage: moving data from one place to another needs to be accompanied by measures to check before and after the move whether the digital object is still complete and undamaged. This also applies to back up copies.</p> <p style="padding-left: 40px;">Authentication measures to safeguard that personnel cannot make changes to the data stored or (unintentionally) delete (part of) digital objects.</p>
Life cycle stage	Preservation Planning Ingest, Preservation Action, Receive, Storage
Stakeholder	<p>Management: should decide on overall measures to maintain integrity</p> <p>Operational management: should implement the measures</p> <p>Producers: will contribute by supporting integrity measures (for example to send checksums with the digital object)</p>
Cross Reference	Bit preservation, Functional Preservation [migration]
Examples	<p>Parliamentary Records: <i>“The record must be maintained to ensure that it is complete, and protected against unauthorised or accidental alteration. In this Policy, integrity is ensured through the bitstream preservation function [...], and through the provision of metadata to describe all authorised actions undertaken in the course of content and bitstream preservation.”</i></p> <p>URL: http://www.parliament.uk/documents/upload/digitalpreservationpolicy1.0.pdf</p>

Control Policy	<p>Possible control policies might be:</p> <ul style="list-style-type: none"> • All preservation events MUST be recorded • Information on preservation events SHOULD use the PREMIS schema • Information on preservation event MUST include date undertaken, action and agent • The file checksum algorithm MUST be <name of algorithm> • File checksum algorithm SHOULD be run on ingest • File checksum-recalculation date \leq today – 2 years • Ingest checksum SHOULD be the same as recalculated checksum
Questions to foster discussions	<ul style="list-style-type: none"> • Does your organisation negotiate with the producer or deliverer of the digital material for checksums to be delivered with the digital material in order to be able to compare checksums once the material has been delivered? • Is your organisation willing to accept the delivery of digital material without a checksum? • Will your repository create their own checksum on receiving digital objects? • Does your repository have procedures implemented to regularly check the checksums? • Does your repository have procedures to handle checksums in preservation actions?

5.2. Preservation Procedure Policy: Reliability	
Related Guidance Policy	Authenticity
Definition/ Description	Reliability is <i>“The trustworthiness of a record as a statement of fact. It exists when a record can stand for the fact it is about, and is established by examining the completeness of the records form, and the amount of control exercised on the process of its creation ”</i> (Source: Alliance for Permanent Access) Often related to the archival community.
Why	Establishing trust in the record keeping and archival processes
Risks	Losing trust in the preserved object
Life cycle stage	Appraise and select
Stakeholder	Management: set requirements Producer: will show meeting the requirements Regulator: will do the actual checking Collection Manager (non Shaman): support management from point of view related to the content to be preserved digital objects
Cross Reference	Bit preservation, Functional Preservation (migration, emulation), Provenance
Examples	Parliamentary Archives : <i>“All preservation strategies will be fully documented via metadata and documentation that will be saved in the repository”</i> <i>“The record must be a full and accurate representation of the business activity to which it attests. This requires the establishment of trust in the record keeping and archival processes used to manage the record throughout its lifecycle, and the continued ability to place the record within its operational context ”</i> Source:, http://www.parliament.uk/documents/upload/digitalpreservationpolicy1.0.pdf
Control Policy	Possible control policies might be: <ul style="list-style-type: none"> • All preservation events MUST be recorded • Information on preservation events SHOULD use the PREMIS schema • Information on preservation event MUST include date undertaken, action and agent
Questions to foster discussions	<ul style="list-style-type: none"> • How do you convince your users that the preserved objects are “reliable”? • What types of information about the digital object does your user community expect to have to enable them to trust the reliability of the object

5.3. Preservation Procedure Policy: Provenance	
Related Guidance Policy	Authenticity
Definition/ Description	<p>Provenance can be defined as: “Documentation of processes in a Digital Object’s life cycle. Digital Provenance typically describes Agents responsible for the custody and stewardship of Digital Objects, key Events that occur over the course of the Digital Object’s life cycle, and other information associated with the Digital Object’s creation, management, and preservation.” (Source: Premis 2.2) This Provenance information is often described in preservation metadata.</p> <p>Knowing the designated community and their requirements is an essential guide for determining which elements of provenance will establish authenticity for them. A set of research data without information on the software and related parameters used to create those research data might infringe the authenticity for a researcher. Lack of information about the original publisher of an e-book might make the digital object useless for a literature researcher.</p> <p>It is not only important to know which elements are important for the Designated Community - the (future) users of the digital material, but these elements need to be recorded as well and verified by them.</p> <p>The provenance trail might differ for different sets of digital objects. For research data this might be links to the analysis process/raw data/publications, etc., for legal deposit libraries this might be the moment when the publisher delivers the digital objects.</p> <p>Provenance will also play a role in preservation actions like Migration and Normalization (see chapter 7.2)</p>
Why	<p>“[Provenance] <i>This ensures that the actions applied to that representation are documented in sufficient detail for present and future users to understand their nature and consequences.</i>” (Source: Premis 2.2). This is also called Provenance information and is often described in preservation metadata.</p>
Risks	Provenance missing may lead to loss of trust by the Designated Community / stakeholders
Life cycle stage	Preservation Planning, Community Watch and Participation, Description & Representation Information, Ingest, Receive Data
Stakeholder	<p>Management: set requirements</p> <p>Producer: will show meeting the requirements</p> <p>Regulator: will do the actual checking</p> <p>Collection manager (non Shaman): support management from point of view related to the content to preserve</p>
Cross Reference	Metadata, Functional Preservation (Migration)
Examples	Parliamentary Archives: “ <i>Maintaining a full audit trail of all preservation actions performed on a representation of a record.</i> ” “Source;,”

6. Guidance Policy: Bit Preservation

As described in the article *A Holistic Approach to Bit Preservation* bit preservation is defined as “*The required activities to ensure that the bit-streams remain intact and readable*”¹. Functional preservation builds upon the results in bit preservation, so it is important that an organisation is aware of this relationship. Bit preservation is not only about preserving the bits, but also to ensure access to the digital material over time. Bit preservation cannot stand alone, it requires also activities to ensure the understandability of the digital material over time.

Policy Elements in this chapter

- 6.1 Define Bit preservation
- 6.2 Define Bit preservation levels
- 6.3 Decide on Ingest activities
- 6.4 Develop Integrity Measures
- 6.5 Assign Persistent Identifiers
- 6.6 Decide on number of copies, geographical distribution and organizational distribution
- 6.7 Define Policy for Disaster Recovery

¹ E.M.Olmütz Zierau: *A Holistic Approach to Bit Preservation*. Thesis 2011, Hvidovre p. 10

6.1. Preservation Procedure Policy: Define Bit preservation	
Related Guidance Policy	Bit preservation
Definition/Description	The organisation should define its understanding of bit preservation and the relation to functional preservation. This bit preservation definition may include topics such as bit integrity measures, different storage locations, regularity of checks, costs, safety levels etc.
Why	A clear definition of the organisation's understanding of the extent of bit preservation ensures that all relevant activities are accounted for. This should not be restricted to a reference to technical information about the storage capacities, but should embrace issues such as bit preservation level, error correction procedures, disaster recovery procedures etc.
Risks	Not defining the organisation's understanding of the extent of bit preservation may endanger the digital material as procedures and responsibilities are unclear.
Life cycle stage	Preservation Planning, Curate and Preserve
Stakeholder	Management: defining bit preservation should be a policy action. Depositor: needs to know that bit preservation and safety measures are performed properly Regulator: concerned with the safety measures in bit preservation
Cross Reference	Functional preservation Metadata Authenticity Access policies, related to the availability of the material, accessible and usable Organisation
Examples	The Royal Library, Denmark: <i>"Bit preservation consists of secure storage of the physical bit sequence, here to be understood as storage in systems with well-established risks, as well as control of integrity and error correction."</i> Source:, http://www.kb.dk/export/sites/kb_dk/da/kb/downloadfiler/PreservationPolicyDigitalMaterials_21092012.pdf
Control Policy	The control policies that reflect what bit preservation means in practice in the organisation will be generated though decisions made in other parts of this section.
Questions to foster discussions	<ul style="list-style-type: none"> Has your organisation defined which activities will encompass bit preservation for the collection (s)?

6.2. Preservation Procedure Policy: Define Bit preservation levels	
Related Guidance Policy	Bit preservation
Definition/Description	<p>The PREMIS definition of “preservation levels” is “Information indicating the decision or policy on the set of preservation functions to be applied to an object and the context in which the decision or policy was made.” (chapter 1.3)</p> <p>The organization might differentiate between different levels of bit preservation, depending on various criteria.</p> <p>A criterion could be based on the distinction of whether it concerns digitized material: preservation copies and/or access copies, or digital born material. For example for the digital born national deposit material, higher levels might be required compared to digitized material of which the analogue version is also preserved. Digital objects preserved for access might require a different bit preservation level than preservation copies, for example because access copies need to be presented faster and often are created in a lower resolution than a preservation copy.</p> <p>Another criterion in defining bit preservation levels might be the value of the digital objects to the collection. If the digital material is absolutely unique and irretrievable from anywhere else in the world in case of loss or errors a high level of bit preservation (e.g. four copies in very distant places with a high frequency of integrity check etc.) would be preferable.</p>
Why	In order to ensure the optimal storage capacity and safety level over time it is vital to be aware of the bit preservation level(s) in the repository.
Risks	Unawareness of bit preservation levels may endanger the digital material as the repository may run out of storage capacity or underestimate the need for safety for specific collections.
Life cycle stage	Preservation Planning
Stakeholder	<p>Management: defining bit preservation could be a policy act</p> <p>Depositor: needs to know that bit preservation and safety measures are performed properly</p> <p>Regulator: concerned with the safety measures in bit preservation</p>
Cross Reference Examples	<p>Functional preservation</p> <p>The Royal Library, Denmark: “For every collection there must also be a decision with regard to level of preservation, including i.e. bit preservation and encrypting.” Source: http://www.kb.dk/export/sites/kb_dk/da/kb/downloadfiler/PreservationPolicyDigitalMaterials_21092012.pdf</p>
Control Policy	<p>Defining a formal bit preservation level, as for example NDSA have done (see below), will generate an appropriate set of control level policies to implement that level of preservation. So taking Level 1 and Level 3 as examples:</p> <p>Level 1</p> <ul style="list-style-type: none"> Number of copies of the data = 2

	<ul style="list-style-type: none"> • Location of copies MUST be in different locations/buildings • File checksum algorithm should be run on ingest • File checksum algorithm MUST be <value> • File format SHOULD be Open Source • File format SHOULD be able to be identified <p>Level 3</p> <ul style="list-style-type: none"> • Number of copies of the data ≥ 3 • Location of copies MUST be different • Location risk for location 1 MUST be different to Location risk for location 2 or location 3 • File checksum algorithm should be run on ingest • File checksum algorithm MUST be <value> • Filechecksum-recalculation date \leq today – 2 years • File format SHOULD be Open Source • File format SHOULD be able to be identified • File format MUST be widely used
Questions to foster discussions	<ul style="list-style-type: none"> • Has your repository defined bit preservation levels for the various parts of the collection? • Does your organisation know what needs different collections/parts of the collection have? • Has your organisation clearly estimated the value of the collection?

6.3. Preservation Procedure Policy: Decide on Ingest activities	
Related Guidance Policy Definition/ Description	<p>Bit preservation</p> <p>In the process of ingesting digital objects into the repository in order to perform bit preservation a number of ingest activities will have to be performed to ensure that the digital material will meet the requirements set by the organisation.</p> <p>For bit preservation there is a minimal set of measures that should be developed. The organisation needs to:</p> <ul style="list-style-type: none"> • ensure that the digital objects are free of viruses by examining the objects before ingest, • ensure that the collection and the objects are complete • identify, characterise and validate formats. <p>Knowing which file formats are in the repository is a cornerstone in digital preservation, as many of the identified risks are related to file formats. There are a variety of tools available to check the file format of digital objects, albeit with different success. The minimal level, but not trustworthy, is identifying file formats based on the file extension and this can be extended with analysis with more trustworthy tools (see Further Reading) Identification could be extended with characterization and validation of the file format, which will give a more complete picture of the content of the repository.</p>
Why	To be able to ensure the integrity of the digital material in the repository it is important that the digital material at time of ingest meets the requirements of the organization and that the organization will have knowledge of what kind of materials are actually ingested.
Risks	Not performing a minimal set of ingest activities may endanger the integrity of the digital material in the repository. Not knowing the file formats might lead to a risk that certain files will no longer be accessible with contemporary tools or tools that are in use by the Designated Community. It also hinders identifying risks connected to the file formats stored.
Life cycle stage	Create or Receive, Description & Representation Information
Stakeholder	<p>Technology Manager: responsible for ensuring the proper systems for bit preservation</p> <p>Operational Manager/Information Operator/System Architect/Technology Operator/Solution Provider : responsible for administrating systems and performing bit preservation</p>
Cross Reference	<p>Functional preservation</p> <p>Metadata</p> <p>Object</p> <p>Organisation – Risk management</p> <p>Access? Authenticity?</p>
Examples	British Library: <i>"Ingest valid legacy digital content into our long term repository..."</i> Source:

Control Policy	http://www.bl.uk/aboutus/stratpolprog/collectioncare/discovermore/digitalpreservation/strategy/BL_DigitalPreservationStrategy_2013-16-external.pdf
	<p>For collection x:</p> <ul style="list-style-type: none"> file format MUST be <defined format> file format MUST be automatically verified
Questions to foster discussions	<ul style="list-style-type: none"> Does your organisation's preservation policy describe the various ingest activities and are these activities part of standard ingest procedures? Does your organisation plan to have an ingest process in which file formats of the preserved objects are identified, eventually checked and reported? Does your organisation plan to check for viruses before ingesting digital material into the repository?

6.4. Preservation Procedure Policy: Develop Integrity Measures	
Related Guidance Policy	Bit preservation
Definition/ Description	<p>Integrity or fixity check: <i>“A mechanism to verify that a digital object has not been altered in an undocumented manner. Checksums, message digests and digital signatures are examples of tools to run fixity checks. Fixity information, the information created by these fixity checks, provides evidence for the integrity and authenticity of the digital objects and is essential to enabling trust.”</i> (Source: NDSA)</p> <p>The organisation needs to develop measures to monitor the bit integrity. As in the definition the integrity measures could consists of adding checksums, digital signatures etc. Regular checks need to be planned in order to monitor the situation in the archive.</p>
Why	Bit integrity needs to be checked on a regular basis to ensure that no changes to the digital material have occurred.
Risks	Lack of procedures for integrity measures may cause unnoticed loss of data.
Life cycle stage	Create and , Preservation Planning, Ingest, Preservation Action
Stakeholder	<p>Technology Manager: responsible for ensuring the proper systems for bit preservation</p> <p>Operational Manager/Information Operator/System Architect/Technology Operator/Solution Provider: responsible for administrating systems and performing bit preservation</p>
Cross Reference	<p>Functional Preservation</p> <p>Authenticity</p> <p>Checksum</p> <p>Integrity</p>
Examples	<p>University of Minnesota: <i>“The University Digital Conservancy maintains fixity (bitstream integrity) for all digital objects submitted in the UDC. This is accomplished using a checksum algorithm (MD5) that verifies that the bitstream of a digital object matches its original bitstream (from date of original deposit in the UDC).”</i> Source: http://conservancy.umn.edu/pol-preservation.jsp</p>
Control Policy	<p>For collection Y:</p> <ul style="list-style-type: none"> File checksum algorithm MUST be <value> Filechecksum-recalculation date <= today – 2 years
Questions to foster discussions	<ul style="list-style-type: none"> Does your organisation have written procedures describing the complete procedure for monitoring integrity of the digital objects (plan, do, check, act)? Does your organisation require checksums from the depositor?

6.5. Preservation Procedure Policy: Persistent Identifiers	
Related Guidance Policy	Bit preservation
Definition/Description	<p>Digital material can easily be copied and altered. Assigning a persistent identifier to the digital object will improve its identification and searchability. The persistent identifier, together with other aspects, will also add to the authenticity of the object. It is important that the organisation develops a policy related to the assignment of the persistent identifiers in their collections. In cases where the received objects already have a persistent identifier, the organisation should decide whether they add their own as well. There is a variety of methods for choosing persistent identifiers, see reference to <i>Persistent Identifiers Interoperability Framework</i> of the APARSEN project in Further Reading.</p> <p>To increase the safety the persistent identifier should be stored separate from the digital object itself.</p>
Why	Assigning persistent identifiers to digital material minimize risks of loss caused by loss of identification.
Risks	Not assigning persistent identifiers to digital material endangers the future identification and authenticity of the digital material.
Life cycle stage	Create or Receive, Ingest, Community Watch and Participation, Preservation Planning
Stakeholder	<p>Technology Manager: responsible for ensuring the proper systems for bit preservation</p> <p>Operational Manager/Information Operator/System Architect/Technology Operator/Solution Provider: responsible for administrating systems and performing bit preservation</p>
Cross Reference	<p>Functional Preservation</p> <p>Preservation</p> <p>Authenticity, Standards</p>
Examples	<p>State Library of Queensland: “<i>The State Library will record preservation metadata about each digital object and allocate unique persistent identifiers to successfully manage and preserve its digital content over time.</i>” (Source:, http://www.slq.qld.gov.au/__data/assets/pdf_file/0020/109550/SLQ_-_Digital_Preservation_Policy_v0.05_-_Oct_2008.pdf)</p>
Control Policy	<ul style="list-style-type: none"> • All files MUST have a persistent identifier • The persistent identifier scheme SHOULD be <value>
Questions to foster discussions	<ul style="list-style-type: none"> • Has your organisation planned for measures on how to assign a persistent identifier to every digital object in the repository? • Has your organisation decided which persistent identifier methodology suits their

domain best (DOI-publishers, NBN-libraries etc.)

- Has your organisation decided how to treat the persistent identifier already in the object?
- Will the persistent identifier be part of the search facilities for the digital object?

6.6. Preservation Procedure Policy: Decide on number of copies, geographical distribution and organisational distribution	
Related Guidance Policy	Bit Preservation
Definition/ Description	One of the approaches in mitigating the risk of data loss is creating copies of the digital material distributed on different technology (e.g. one copy on tapes and one copy on disks), stored in different geographical locations and administered by different staff or organisations. It is important that active bit preservation takes place, including regular checks between the different copies etc. Sometimes there are restrictions to the geographical location where the copies can be stored, either legally (not out of the country) or practically (e.g. in the cloud or with external parties).
Why	In order to keep data safe it is vital to avoid single points of failure. This can be avoided by making more copies, storing the copies in different locations and on different hardware/media and administering it by different staff.
Risks	Keeping only one copy of digital material or keeping multiple copies in the same location endangers the preservation of the digital material as there will be single points of failure.
Life cycle stage	Preservation Planning, Store
Stakeholder	Technology Manager: responsible for ensuring the proper systems for bit preservation Operational Manager/Information Operator/System Architect/Technology Operator/Solution Provider: responsible for administrating systems and performing bit preservation
Cross Reference	Functional Preservation Trustworthy Digital Repository
Examples	State and University Library, Denmark: <i>"The two copies will be stored by using different technologies, and the library makes sure that both copies are not controlled by the same organisational unit and/or person."</i> (Source: http://en.statsbiblioteket.dk/about-the-library/dpstrategi)
Control Policy	For collection x: <ul style="list-style-type: none"> No-of-copies = 3 No-Geographic locations ≥ 3 Geographic locations SHOULD be in EU For collection z <ul style="list-style-type: none"> No-of-copies = 4 No-Geographic locations = 4 Outsourcing IS allowed
Questions to foster discussions	<ul style="list-style-type: none"> Does your organisation have procedures in place for duplication of digital material in the repository?

- Does your organisation have procedures in place for storing copies in different geographical locations with different staff affiliated to the different copies?
- Does your organisation have planned budget for the bit preservation activities?
- Does your organisation have plans in place for monitoring the integrity between the copies?

6.7. Preservation Procedure Policy: Defining Policy for Disaster Recovery	
Related Guidance Policy	Bit preservation
Definition/ Description	When performing bit preservation it is vital to have a policy describing the measures taken in relation to whether disaster recovery procedures are in place and tested. The organisation needs to know what to do when data loss occurs, e.g. caused by bit rot, natural disaster or accident. The loss could be discovered by regular checksum checks. Procedures need to be in place for how the organisation will decide which copy is intact and which is damaged, who should make the final decision for what to preserve and what to discard of, and how new authoritative copies are created. This is very much related to IT processes in the organisation.
Why	To keep the integrity of the digital material in the repository intact it is important to react promptly and appropriately when bit errors occur and a policy on this issue could help prevent total loss.
Risks	Lack of recovery procedures endangers the integrity of the digital material and the trustworthiness of the repository.
Life cycle stage	Curate and preserve, Store
Stakeholder	Technology Manager: responsible for ensuring the proper systems for bit preservation Operational Manager/Information Operator/System Architect/Technology Operator/Solution Provider: responsible for administrating systems and performing bit preservation
Cross Reference	Functional Preservation Trustworthy Digital Repository Authenticity Organisation – Risk Management
Examples	UK Data Service (2012): “Disaster Recovery Procedures are in place” (Source: http://data-archive.ac.uk/media/54776/ukda062-dps-preservationpolicy.pdf) Wellcome Trust Preservation Policy: “The Library Business Continuity Team is responsible for ensuring that contingency plans and procedures are in place to prevent, react to and recover from emergency situations that may have an adverse effect on the Library collections. Details of Disaster Preparedness, Asset Recovery and prevention procedures can be found in the Wellcome Trust’s Business Continuity Plan.” (Source: http://wellcomelibrary.org/content/documents/policy-documents/preservation-policy)
Control Policy	Once the procedures as described are in place, it would be possible to generate specific control policies.

<p>Questions to foster discussions</p>	<ul style="list-style-type: none"> • Has your organisation defined a policy for disaster recovery procedures? • Has your organisation procedures in place for deciding which copy is intact and which damaged in case of disaster?
--	--

7. Guidance policy: Functional Preservation

Functional preservation, also known as content preservation or logical preservation: “(...) seeks to ensure the continued accessibility of digital resources over time, by active intervention to minimise the disruption caused by technological changes. It may generate new technical versions of the resources through processes such as format migration. These new versions are then incorporated into the preservation storage environment for ongoing bitstream preservation.” (Source: [Parliamentary Archives](#))

Functional preservation covers a number of different preservation strategies all aiming at preserving different kinds of digital material. Choosing a functional preservation strategy needs careful consideration as a strategy needs to be selected that preserves the integrity of the material after preservation actions and allows the organisation and the Designated Community to access and understand the material for years to come.

Policy elements in this chapter

- 7.1 Plan functional preservation
- 7.2 Define preservation strategies
- 7.3 Define Ingest activities / preservation actions
- 7.4 Keep track of versions when performing migration

7.1. Preservation Procedure Policy: Plan functional preservation	
Related Guidance Policy	Functional preservation
Definition/Description	<p>A number of factors or conditions may influence the choice of preservation strategy; these factors can be both organisational and technical</p> <p>The organisation needs to consider a number of issues before entering into functional preservation such as:</p> <ul style="list-style-type: none"> • Technological changes: the major driver for accessing and understanding the digital material in the future. • Risks: the organisation needs to be aware of the risks that can affect the future understanding of the digital material. The organisation also needs to decide the “risk appetite” of the organisation i.e. how much risk the organisation is prepared to take? These could be technological risks, e.g. format obsolescence, lack of sufficient tools to perform the preservation actions properly etc., or organisational risks e.g. budget cuts, insufficient technical expertise etc. • The needs of the Designated Community - what do they need in order to be able to access and understand the digital material in the short and the long term? • The use of standards – the organisation needs to decide if and what standard to use.
Why	The organisation should consider all current technological and organisational risks to be able to ensure continued long term access to the digital collection.
Risks	Uncertainty about the factors and risks affecting the functional preservation could endanger the continued preservation of and access to the digital collection.
Life cycle stage	Preservation Planning
Stakeholder	<p>Depositor: the organization needs to ensure continued accessibility of the digital material</p> <p>Consumer: has an interest in continued accessibility of the digital material</p> <p>Information Manager: has to decide on policies for functional preservation</p> <p>Technology Manager/System Architect: have to provide technology solutions for functional preservation</p>
Cross Reference	<p>Costs</p> <p>Bit Preservation</p> <p>Standards</p> <p>Digital Object</p>
Examples	<p>The Royal Library, Denmark: “<i>Logical [functional] preservation must safeguard the digital materials against technological obsolescence, so that both now and in the future will be able to read, understand and display/play the materials with standard programs and equipment.</i>” (Source: http://www.kb.dk/export/sites/kb_dk/da/kb/downloadfiler/PreservationPolicyDigitalMaterials_21092012.pdf)</p>

Control Policy	<p>In preparation for creating control policies, the organisation may identify:</p> <ul style="list-style-type: none"> • The possible user communities/roles This could be very specific or at a minimum can relate to one of three roles: creator; manager/curator and end user. • The collections which will need different preservation strategies • The risks for which mitigation actions have to be defined • General approach to the use of standards. <p>Some of these results will be used in formulating the preservation cases, and some will be used for control policies themselves.</p> <p>An example of a control statement would be:</p> <ul style="list-style-type: none"> • All metadata describing preservation activities MUST comply with the PREMIS standard.
Questions to foster discussions	<ul style="list-style-type: none"> • Does your organisation have a plan for functional preservation? • Has your organisation considered how technological change will effect long term preservation? • Has your organisation considered the risks to the future understanding of the digital material? • Has your organisation considered the needs of the user community?

7.2. Preservation Procedure Policy: Define preservation strategies	
Related Guidance Policy	Functional preservation
Definition/Description	<p>Describing the organisational elements that can influence the level and type of digital preservation and defining the significant properties (see Chapter 8.5 Significant properties) of the digital material enables the organisation to decide on the proper functional preservation strategy as listed below. The list reflects today's options but technologies may shift rapidly and new technical solutions may emerge.</p> <p>Migration</p> <p>Migration is a functional preservation strategy that transforms obsolete or soon to be obsolete formats into more viable formats. Migration can also be performed before ingest of digital material into the repository in order to normalize file formats to be able to limit the amount of different file formats in the repository. When an organisation chooses to apply a migration strategy the organisation should decide when the migration should take place. It could either be before ingest (normalization) or when the format is at risk of becoming obsolete (just-in-time migration). If just-in-time migration is decided upon the organisation should watch the development of file formats carefully.</p> <p>Emulation</p> <p>Emulation is a functional preservation strategy that preserves the digital material in the original file format and develops software tools that can simulate the original software needed to access the digital material. When choosing emulation as functional preservation strategy, planning and resourcing of how the organisation will either develop or implement emulation tools in the repository should be carried out.</p> <p>Software/hardware archiving</p> <p>When doing software/hardware archiving the organisation preserves the original hardware and software to be able to access the digital material in the original environment. If the organisation should decide upon this solution the organisation should consider how to be able to maintain the archival software and hardware in the long term.</p> <p>Filming</p> <p>If the organisation deems it to be unrealistic to preserve an interactive collection by emulation or migration, but the organisation still finds the collection to be of such value that certain properties of the collection must be preserved, filming use and content of the interactive collection could be a way of preserving significant properties of that collection. This could be done when dealing with e.g. online multi-player games or interactive websites.</p> <p>It could benefit the organisation to document in the preservation procedure policies which preservation strategies the organisation would prefer and in what</p>

	instances a secondary preservation strategy comes into action, e.g. it could be that the organisation chooses migration as its primary preservation strategy but in case of migration not being cost effective or a migration path that preserves the significant properties cannot be found emulation is the secondary choice.
Why	Choosing a preservation strategy after defining both organisational and technological factors and significant properties enables the organisation to perform consistent and viable long term functional preservation.
Risks	The risk of losing either access to the digital collection or comprehensibility of the digital collection is impending if the organisation neither performs functional preservation at all nor performs functional preservation without analysing both significant properties and influential organisational and technological factors beforehand.
Life cycle stage	Preservation Planning, Preservation Action, Transform, Migrate, Access Use and Reuse
Stakeholder	<p>Depositor: needs to be assured that the organisation ensures continued accessibility of the digital material</p> <p>Consumer: have an interest in continued accessibility of the digital material</p> <p>Information Manager: has to decide on functional preservation strategies</p> <p>Technology Manager/System Architect: have to provide technology solutions for functional preservation</p>
Cross Reference	<p>Bit preservation</p> <p>Access</p> <p>Digital object (significant properties)</p>
Examples	<p>Bayerischen Staatsbibliothek: "Derzeit wird dabei die Migration in aktuelle, standardisierte und offene Dateiformate als wichtigste digitale Erhaltungsstrategie erachtet, es besteht aber eine grundsätzliche Offenheit gegenüber anderen Maßnahmen (z. B. Emulation)." (Source:http://www.babs-muenchen.de/content/dokumente/2012-11-22_BSB_Preservation_Policy.pdf)</p> <p>National Archives of Australia: "The Archives converts digital records to fully-specified, standards-based open formats (that is, formats whose specification is fully and openly published). The conversion occurs when the records are ingested into the Digital Archive. This is a 'migration' approach to digital preservation that limits the number of preservation treatments applied to each digital record, thereby minimising the risk of altering or damaging the record." (Source:, http://www.naa.gov.au/about-us/organisation/accountability/operations-and-preservation/digital-preservation-policy.aspx#section7)</p>
Control Policy	<p>Once the significant properties have been established – for example that the experience of watching a moving image should be the same after preservation, this can be described using the specific measureable aspects of the file & its contents.</p> <p>An example for a collection of MPEG2 files, the following control policies might set some of the significant properties:</p> <ul style="list-style-type: none"> • File format MUST be MPEG2

	<ul style="list-style-type: none"> • The height of the video track ≥ 586 • Image width of the video ≥ 720 • Video bitrate ≥ 6000 <p>Whereas an example for a collection of digitized newspapers might include:</p> <ul style="list-style-type: none"> • Colour model preserved MUST be TRUE • Compression type MUST be NONE
Questions to foster discussions	<ul style="list-style-type: none"> • Has your organisation defined the significant properties that should be preserved? • What is your organisation's approach to digital objects which have been transformed – will the original digital object be disposed of? If not, will an end user be able to choose which version of the digital object they access? • Has your organisation defined the process for choosing the most effective preservation strategy? • How does your organisation compare alternative strategies? • Has your organisation decided upon a strategy for which digital copy/copies an end user can access?

7.3. Preservation Procedure Policy: Define Ingest activities / preservation actions	
Related Guidance Policy	Functional preservation
Definition/Description	To be able to secure the long term preservation of the digital material it is necessary to validate and characterise file formats before ingest into the repository (or before and after migration). The organisation should also obtain the necessary metadata generated during these actions.
Why	Proper ingest activities/preservation actions ensure that the content and condition of the digital collection are well known and therefore easier to make the best digital preservation choices for.
Risks	Refraining from validation, characterisation and obtaining of proper metadata endanger the preservation of the digital collection both in the short and long term as the organisation will not be able to act according to the needs of the collection.
Life cycle stage	Create or Receive, Ingest, Preservation Action
Stakeholder	Technology Manager/System Architect: have to provide technology solutions for functional preservation
Cross Reference	Bit preservation Metadata Preferred Format
Examples	UK Parliamentary Archives: <i>“Digital resources which are selected for preservation will be accessioned into an appropriate preservation environment. The process of accessioning encompasses both steps to bring those resources under intellectual control (e.g. cataloguing and transfer of custody), and the more technical processes of ingest, which may include characterisation (see 5.5.1), quarantine, validation, and the physical transfer of digital objects and metadata into a digital repository environment.”</i> (Source; http://www.parliament.uk/documents/upload/digitalpreservationpolicy1.0.pdf)
Control Policy	For ingest: <ul style="list-style-type: none"> • Format Identification MUST be possible • Format validation SHOULD be automatic • Format MUST be an ISO standard • The file checksum algorithm MUST be <name of algorithm> • File checksum algorithm SHOULD be run on ingest
Questions to foster discussions	<ul style="list-style-type: none"> • Has your organisation defined which ingest activities / preservation actions to perform? • Does your organisation have a plan for obtaining metadata from ingest activities / preservation actions?

7.4. Preservation Procedure Policy: Keep track of versions when performing migration	
Related Guidance Policy	Functional preservation
Definition/Description	<p>The organisation needs to decide whether to preserve or dispose of originals when digital material has been migrated. This decision should be part of the digital preservation policy for the organisation. The choice of preserving or disposing depends on a number of factors, i.e. the organisational and technological factors already defined.</p> <p>The decision of preserving or disposing of intermediate or previous versions after a migration can be influenced by factors such as cost, storage capacity, and resources to administer the digital material etc.</p> <p>Also the question of the demands from the Designated Community should be taken into account. For instance does the Designated Community demand access to both originals and migration copies to be able to verify the authenticity of the material or do they trust that the organisation has performed a migration which is true to the original material?</p> <p>The organisation should formulate a policy for access and version control to be able to provide the Designated Community with the best possible access opportunities and to keep the authenticity of the material viable.</p>
Why	There will always be a risk of errors occurring during preservation actions such as migration. Therefore it is important that the organisation at least is clear about the decision made on disposing or keeping originals after a migration and keeps track of the different versions to be able to proof the authenticity of the material.
Risks	Future users can suspect that the organisation has willingly or unwillingly disposed of valuable digital material and the organisation may lose its trustworthiness and the material would lose its authenticity.
Life cycle stage	Preservation Planning, Ingest, Preservation Action, Access, Use and Reuse
Stakeholder	<p>Depositor: should be able to rely upon the integrity of the digital material</p> <p>Consumer: should be able to rely upon the integrity of the digital material</p> <p>Management: defines policies for versioning</p> <p>Technology Management/System Architect: develop systems to support versioning requests</p>
Cross Reference	<p>Authenticity</p> <p>Access</p> <p>Trustworthy Digital Repository</p>
Examples	“(…) establish procedures to meet archival requirements pertaining to the provenance, chain of custody, authenticity, and integrity (bit-level and content) of institutional records and assets.” Source: Cornell University Library, http://hdl.handle.net/1813/11230)

Control Policy	<ul style="list-style-type: none"> • All preservation events MUST be recorded • Information on preservation events SHOULD use the PREMIS schema • Information on preservation event MUST include date undertaken
Questions to foster discussions	<ul style="list-style-type: none"> • Has your organisation decided whether to keep or dispose of intermediate versions after migration? • Does your organisation have a plan for securing integrity of the digital material? • Does your organisation know if the Designated Community needs access to both originals and migration copies to be able to trust the digital material? Mentioning important articles related to this element

8. Guidance Policy: Digital Object

Understanding the specifics of your collection and the different relative values of the parts can help with policy decisions around resourcing and preservation activities.

Policy Elements in this chapter

- 8.1 Original Object
- 8.2 Deletion of objects
- 8.3 Keep track of file format developments
- 8.4 Take down policies
- 8.5 Significant properties

8.1. Preservation Procedure Policy: Original object	
Related Guidance Policy	Digital Object
Definition/Description	The National Digital Stewardship Alliance (NDSA) defined the original object as “the primary authentic and unique item, either the original or the closest surviving surrogate or copy, as originally acquired by the Library”. Currently it is called the “received object”. Source: NDSA wiki page
Why	<p>During the life cycle of the digital object various preservation actions might be undertaken in order to keep the originally ingested object accessible and authentic. This could be a preservation action resulting in a new digital object, e.g. through migration of file formats.</p> <p>Although it is common understanding that the original object always will be kept in the repository, and that preservation actions will be done on copies of the original object, this might not be feasible in all situations. An organisation will need to develop a policy that describes how the organisation will deal with migrated copies, for example when several migrations have taken place, only the original object and new version will be saved and no intermediate versions will be kept.</p>
Risks	<p>It should be clear for the Consumer which version of the object the repository will keep.</p> <p>In case of a preservation action, like migration it will be important to know before the action to determine which version(s) of the object will be preserved.</p>
Life cycle stage	Curate and Preserve, Appraise and Select, Ingest, Preservation Action
Stakeholder	<p>Management: will decide on the definition</p> <p>Collection Manager (non Shaman): support management from point of view related to the content to preserve</p>
Cross Reference	Functional Preservation
Examples	<p>National Archive and Library of New Zealand: : “Preservation actions [...] will not directly affect the original item” Source: http://archives.govt.nz/sites/default/files/Digital_Preservation_Strategy.pdf</p> <p>Portico: “Portico will preserve content provider supplied updates to previously supplied content in the archive alongside the original artefact, including original and updated metadata. “Source: http://www.portico.org/digital-preservation/wp-content/uploads/2011/03/Portico-Content-Update-Policy.pdf</p>
Control Policy	<p>For example, for a collection where only the latest and original version are kept:</p> <ul style="list-style-type: none"> • Original version MUST be kept • Version with the latest creation date MUST be kept
Questions to foster discussions	<ul style="list-style-type: none"> • Has your organisation decided on how to deal with migration copies?

8.2. Preservation Procedure Policy: Deletion of objects	
Related Guidance Policy	Digital object
Definition/Description	An organisation might have a policy for disposal or planned deletion of digital objects. This could be a consequence of preservation agreements or for example by legal mandate like in the archival world... It is important that these decisions are recorded appropriately, and in case this is required by the user community, that there is some information that the object has been removed on purpose.
Why	Managed disposal is part of activities required for collection management. There may be specific reasons why the object/collection has been removed, such as a change of remit of the organisation and the collection has been moved, or it might be that the organisation operates a retention and disposal policy.
Risks	Managed deletion of objects ensures that the decisions behind the removal are recorded and there is less risk of objects not being available by error.
Life cycle stage	Dispose
Stakeholder	Management: will decide on the process Collection Management (non Shaman): support management from point of view related to the content to preserve
Cross Reference	Access, Provenance
Examples	<p>National Library of Australia: <i>“(We) Will consider the following broad preservation action approaches that are likely to be required: (...) - Deaccessioning or deletion.”</i> Source: http://www.nla.gov.au/policy-and-planning/digital-preservation-policy</p> <p>UK Data Service Preservation Policy: <i>“In cases of the withdrawal of a data collection, the administrative metadata are updated, and the external view of the catalogue record is updated to reflect the change of status of the collection (with information about why the collection had been withdrawn, dates of its availability, and where appropriate reasons for withdrawal)”</i> Source: http://data-archive.ac.uk/media/54776/ukda062-dps-preservationpolicy.pdf</p>
Control Policy	<p>For an object where it is not actually deleted, but not accessible, the following control policies may be valid:</p> <ul style="list-style-type: none"> All preservation events MUST be recorded <p>In this case access would be managed through the digital object management system.</p>
Questions to foster discussions	<ul style="list-style-type: none"> Is there a policy in place that describes under which circumstances the organisation will delete objects from its collection Is there a policy in place that describes whether and which metadata will be created in case deletion of objects will occur? (for example provenance metadata)

8.3. Preservation Procedure Policy: Keep track of developments of file formats

Related Guidance Policy	Digital object
Definition/Description	Functional preservation of digital objects is about securing as much knowledge as needed about the digital material to be able to preserve and access the material in the long term. Which file formats and versions of file formats that are preserved in the repository could be important metadata for preserving the collection in the long term as this is important knowledge when decisions about e.g. migration are to be made. It is important that the organisation develops a strategy for maintaining information about the file formats and different versions in the metadata that belongs to the digital object and at the same time decides on how the organisation will continuously watch the development of formats (Preservation Watch). If the organisation does not wish to maintain an in-house format registry the organisation could consider keeping track of file format versioning by use of a central format registry.
Why	Keeping track of file format versions is necessary to be able to choose and perform the proper functional preservation actions.
Risks	Not keeping track of file format versions and monitoring formats in general may put the collection at risk as it will be difficult to know how, when and what needs preservation care.
Life cycle stage	Preservation Planning, Community Watch and Participation
Stakeholder	<p>Depositor: needs to be confident that the digital material is properly preserved and accessible for the long term</p> <p>Consumer: depends on the authenticity of the digital material and will have an interest in continued accessibility of the digital material</p> <p>Information Manager: has to decide on policies for functional preservation</p> <p>Technology Manager/System Architect: have to provide technology solutions for functional preservation</p>
Cross Reference	Authenticity, Metadata, Functional Preservation
Examples	National Archives of Australia: <i>"The Archives uses preservation formats selected through a rigorous research and testing regime."</i> Source:, http://www.naa.gov.au/about-us/organisation/accountability/operations-and-preservation/digital-preservation-policy.aspx
Control Policy	<p>File format identification and monitoring can be done through a variety of checks such as:</p> <ul style="list-style-type: none"> • File format MUST be an ISO-Standard • Information about file format version SHOULD be recorded in the metadata • File format for collection x MUST be <value>

Questions
to foster
discussions

- Has your organisation developed a strategy/policy for maintaining information about file format versions?

8.4. Preservation Procedure Policy: Take-down policy	
Related Guidance Policy	Digital Object
Definition/Description	With “Take-down” here is meant that digital objects will no longer be accessible on purpose. There may be circumstances where a digital object and/or collection needs to be removed (either from public sight or from the repository as a whole) as the organisation does for example not hold the rights for it. In these cases a clear take-down policy is required, to show the Designated Community and the Producers how the organization will take action if a service will occur.
Why Receive Data	For the Designated Community it is important to know which collections the organisations has and what policy there is in relation to their future existence.
Risks	Not having a policy for take down or deletion of digital material may endanger the digital material and the legal access to the digital material.
Life cycle stage	Access, use and reuse, disposal
Stakeholder	<p>Management: needs to that there is a process in place</p> <p>Collection managers: need to ensure that appropriate material is ingested</p> <p>Technology Management: needs to ensure that the technical set up can enable successful takedown activities</p> <p>Collection Management (non Shaman): support management from point of view related to the content to preserve</p>
Cross Reference	Functional preservation (ingest) Access
Examples	<p>The UK National Archives: <i>“Material will be taken down temporarily on receipt of a request from a member of the public or a government department. The case will then be considered by a Takedown Panel composed of members of staff who provide relevant expertise. The panel will approve continued withdrawal of the material only if one of the following criteria is met:</i></p> <ul style="list-style-type: none"> <i>• Because of changed circumstances material previously published in good faith is now considered to be subject to an exemption in the Freedom of Information (FOI) Act or the Environmental Information Regulations (EIR) and the public interest lies in withholding it</i> <i>• The material is personal information about someone who is still alive and continued online access would be unlawful or unfair to them under the Data Protection Act 1998 or would breach their or their family's right to a private life under the Human Rights Act 1998</i> <i>• Making the material available online is an infringement of copyright</i> <i>• The material is defamatory or obscene</i> <i>• The material acquires sensitivity through being available online, although an FOI/EIR exemption need not be applied to on-site access to the same information in paper format</i> <i>• Continued online access would cause a department serious and real</i>

	<p><i>administrative difficulties and it has requested takedown for a specified and limited period of time</i></p> <ul style="list-style-type: none"> • <i>The material was released in error and removal is required to rectify a mistake”</i> <p>Source: http://www.nationalarchives.gov.uk/legal/takedown-policy.htm</p>
Control Policy	<p>Occurrences of events which are covered by take-down policies are quite rare, and it is not possible to automatically test for them. However this event needs to be recorded so control policies about take-down policy might include:</p> <ul style="list-style-type: none"> • Information on preservation events SHOULD use the PREMIS schema • Information on preservation event MUST include date undertaken, action and agent
Questions to foster discussions	<ul style="list-style-type: none"> • Does your organisation have a policy in case there is a request to take down material due to copyright infringement? • Does your organization have a policy in case a request to take down material due to privacy matters?

8.5. Preservation Procedure Policy: Define significant properties	
Related Guidance Policy	Digital Object
Definition/Description	<p>To enable the organisation to choose the proper functional preservation strategy it needs to define the significant properties for each type of digital collection to be preserved. The decisions should be documented properly.</p> <p>Significant properties are defined by Jisc as: “(...) <i>essential attributes of a digital object which affect its appearance, behaviour, quality and usability. They can be grouped into categories such as content, context (metadata), appearance (e.g. layout, colour), behaviour (e.g. interaction, functionality) and structure (e.g. pagination, sections). Significant properties must be preserved over time for the digital object to remain accessible and meaningful.</i>” (Source: Jisc)</p> <p>Another expression used these days is “Preservation Intent “, see reference article in Further Reading.</p>
Why	Choosing a preservation strategy after defining significant properties enables the organisation to perform consistent and viable long term functional preservation.
Risks	The risk of losing either access to the digital collection or comprehensibility of the digital collection is impending if the organisation neither performs functional preservation at all nor performs functional preservation without analysing both significant properties and influential organisational and technological factors beforehand.
Life cycle stage	Preservation Planning, Preservation Action, Transform, Migrate, Access Use and Reuse
Stakeholder	<p>Depositor: needs to be assured that the organisation ensures continued accessibility of the digital material</p> <p>Consumer: have an interest in continued accessibility of the digital material</p> <p>Information Manager: has to decide on functional preservation strategies</p> <p>Technology Manager/System Architect: have to provide technology solutions for functional preservation</p>
Cross Reference	<p>Bit preservation</p> <p>Functional preservation</p> <p>Access</p>
Examples	<p>National Library of Wales: <i>In implementing this policy with regard to its own collections, NLW will: [...] Define the significant properties that need to be preserved for particular classes of resources.</i> “Source http://www.llgc.org.uk/fileadmin/documents/pdf/2008_digipres.pdf</p>
Control Policy	Once the significant properties have been established – for example that the experience of watching a moving image should be the same after preservation,

<p>Questions to foster discussion</p>	<p>this can be described using the specific measureable aspects of the file & its contents.</p> <p>An example for a collection of MPEG2 files, the following control policies might set some of the significant properties:</p> <ul style="list-style-type: none"> • File format MUST be MPEG2 • The height of the video track ≥ 586 • Image width of the video ≥ 720 • Video bitrate ≥ 6000 <p>Whereas an example for a collection of digitized newspapers might include:</p> <ul style="list-style-type: none"> • Colour model preserved MUST be TRUE • Compression type MUST be NONE <div> <ul style="list-style-type: none"> • Has your organisation defined for each collection the significant properties that should be preserved? • Have you involved all the stakeholders in your organisation to define the significant properties? </div>
---------------------------------------	--

9. Guidance policy: Metadata

Metadata is data about data and is a core issue in digital preservation. Metadata adds value to the data that needs to be preserved and is used for describing, administering and retrieving data. In digital preservation several kinds of metadata need to be created and maintained.

Some metadata will be created by the producer of the digital object, often called “original metadata” and during the digital life cycle other metadata will be added by the organization before the digital objects will be ingested into the repository. It is important that the organisation defines its policies for metadata.

The original metadata that comes with the digital object files must be kept to ensure provenance and authenticity of the digital objects and can be of many different kinds. These metadata will be static compared to other types of metadata that can be generated and extended when or after the digital collection is deposited.

Besides the original metadata using with the metadata types below would be advisable. Descriptive metadata or bibliographic metadata is used for describing the collection or the digital object (who, what, when, where etc.). The preservation metadata (administrative metadata, technical metadata, rights management metadata etc.) describes information that are needed to be able to perform long term preservation of the digital collection, e.g. origin, digitization metadata, technical environment necessary to maintain access to the digital object etc. Structural metadata contains information on how to understand the digital object including what file types a digital object consists of etc.

To these different kinds of metadata different standards apply. For descriptive metadata e.g. MODS, DCMI or MARC are well known standards. For preservation metadata the standards PREMIS and MIX among others can be used, and for structural metadata METS is an example of a useful standard.

Content

- 9.1 Management of Metadata
- 9.2 Original Metadata
- 9.3 Types of metadata
- 9.4 Descriptive Metadata
- 9.5 Preservation Metadata
- 9.6 Structural Metadata

9.1. Preservation Procedure Policy: Metadata: Management of metadata	
Related Guidance Policy	Metadata
Definition/ Description	<p>An organisation undertaking digital preservation should develop a metadata policy describing what kind of metadata and which standards are to be used. This policy would support decision making for preservation of specific collections.</p> <p>As the required set of metadata can differ per collection or type of digital object, the organisation should decide for each kind of digital collection what type of metadata the organisation will need for long term digital preservation taking into consideration the users of that collection and the preservation goals.</p> <p>It would be beneficial to consider using agreed standards for the different types of metadata. Whether standards are followed or not, it will be important to document all decisions and review on a regular frequency to update for developments in standards and demands for preservation.</p>
Why	A policy for metadata, use of metadata standards and consideration of management of metadata are necessary to support a successful long term digital preservation.
Risks	Lack of policies for collection and management of metadata may cause that metadata that is often recorded at a certain point in time (e.g. at the point of creation of the file or at time of ingest) is not collected or managed appropriately.
Life cycle stage	Preservation Planning, Create or Receive, Ingest, Preservation Action, Store, Dispose, Transform
Stakeholder	<p>Depositor: delivers metadata for long term preservation</p> <p>Management: decides overall metadata policies and standards</p> <p>Regulator: concerned with the legalities in metadata</p>
Cross Reference	<p>Functional Preservation</p> <p>Authenticity -> Provenance</p> <p>Trustworthy Digital Repository</p> <p>Object (original metadata and Dispose)</p>
Examples	<p>University of Manchester Library “ (...)ensure that access is provided for digitally archived objects using appropriate metadata standards (within recognised IP and data protection restrictions)” Source:, http://www.library.manchester.ac.uk/aboutus/strategy/ files2/Digital-Preservation-Strategy.pdf</p> <p>State and University Library, Denmark: “The owner of the digital collections is responsible for defining a minimum level for metadata (...)” Source:, http://en.statsbiblioteket.dk/about-the-library/dpstrategi</p>
Control Policy	<ul style="list-style-type: none"> • Metadata MUST comply with a standard schema <value> • Minimum metadata fields MUST be completed

<p>Questions to foster discussions</p>	<ul style="list-style-type: none"> • Has your organisation defined a metadata policy for long term preservation of digital material? • Has your organisation decided what kind of metadata the organisation will need for long term digital preservation for each collection? • Does the metadata collected and used conform to agreed standards and are the standards used up to date? • Is the metadata about the digital material kept separate from the digital object or is it embedded in the digital object itself? • Has your organisation defined a minimum set of required metadata?
--	---

9.2. Preservation Procedure Policy: Metadata: Original metadata	
Related Guidance Policy	Metadata
Definition/ Description	<p>The term “original metadata” means metadata that is with the digital object at the time it is received by the repository and can consist of different kinds of metadata. This original metadata should be preserved along with the digital object to ensure provenance and authenticity. The organization should have a policy describing how they intend to collect (e.g. by agreement with the depositor or producer) and manage these original metadata.</p> <p>It could be beneficial to develop a policy with regard to agreements with the depositor about which metadata would be preferable and expected, e.g. technical metadata about hardware and software used in the process of creating the digital objects. The repository should safeguard all relevant metadata in the submission package, where “relevant” implies metadata that can only be created by the producer and cannot be derived from the digital object itself.</p>
Why	Original metadata can add to the provenance and authenticity of the digital object. Often this kind of metadata contains information that cannot be retrieved authentically from other sources.
Risks	Not keeping the original metadata or unrecorded manipulation might lead to loss of authenticity and provenance.
Life cycle stage	Description and Representation Information, Preservation Planning, Create or receive, Ingest
Stakeholder	<p>Depositor: delivers metadata</p> <p>Consumer: needs to be able to access and trust the metadata in order to understand the digital material</p>
Cross Reference	Authenticity Provenance Object
Examples	<p>State Library of Queensland: “As some digital preservation activities may result in changes to the digital material all digital preservation processes will be documented in the provenance metadata to ensure the authenticity of the digital records.” Source: http://www.slq.qld.gov.au/__data/assets/pdf_file/0020/109550/SLQ_-_Digital_Preservation_Policy_v0.05_-_Oct_2008.pdf</p> <p>State and University Library, Denmark: “In connection with digitisation, documentation should include relevant metadata, including data generated during the digitisation process.” Source: http://en.statsbiblioteket.dk/about-the-library/dpstrategi</p>
Control Policy	<ul style="list-style-type: none"> • Information about object creation MUST be kept • Ingest event information MUST be recorded • Information on ingest event MUST include date undertaken,

Questions to
foster
discussions

- How does your organisation manage metadata that is received along with the digital object?
- Has your organisation defined a policy to support the process of selecting “relevant original metadata “at ingest?

9.3. Preservation Procedure Policy: Metadata: Descriptive metadata	
Related Guidance Policies	Metadata
Definition/Description	Descriptive metadata is related to the OAIS term `Descriptive information` and supports the user in finding the digital objects. Descriptive metadata is used for describing the collection and digital objects within this collection (who, what, when, where etc.) to be able to identify and retrieve the digital material in the future. It is in the descriptive metadata that the intellectual content of each digital object is described. The organisation should use a standard to be able to retrieve the information about the digital collection. The organisation should define a set of minimum fields from a metadata standard scheme that must be filled in for each digital object. It is also important to be aware of any domain specific information that needs to be included in the descriptive metadata.
Why	A minimum set of descriptive metadata is necessary in order to understand and retrieve the digital object. The information about a digital object needs to be findable in order to be accessible.
Risks	Lack of descriptive metadata can make it impossible for a future designated community to find and comprehend the digital object.
Life cycle stage	Description & Representation Information, Preservation Planning, Create or Receive, Ingest, Access Use, and re-use
Stakeholder	Management: defines metadata policies and the use of standards Technology Manager: responsible for ensuring the proper systems for rendering the metadata and the digital material Consumer: needs to be able to access and trust the metadata in order to understand the digital material
Cross Reference	Designated Community Access Authenticity Standards Interoperability Usability
Examples	<p>Swiss Federal Archives: <i>"The SFA archive information system (AIS) for the management of description information (administrative, descriptive, structural and technical metadata) guarantees the retrievability of documents independently of the type of archive records."</i> Source: http://www.bar.admin.ch/themen/00876/index.html?lang=en&download=NHzLpZeg7t,lnp6lONTU042l2Z6ln1ad1lZn4Z2qZpnO2Yuq2Z6gpJCDdYB,fmym162epYbg2c_JjKbNoKS6A --📄</p> <p>Wellcome Library: <i>"The Library considers metadata (Technical as well as descriptive) to be essential for lifecycle management as well as resource discovery."</i> Source: http://wellcomelibrary.org/content/documents/policy-documents/preservation-policy</p>

Control Policy	<ul style="list-style-type: none"> • Schema used for descriptive metadata SHOULD be Dublin Core • Minimum metadata fields MUST be completed <p>For collection x with digitized newspapers then</p> <ul style="list-style-type: none"> • Metadata MUST include scanning device
Questions to foster discussions	<ul style="list-style-type: none"> • Does your organisation use a standard(s) for descriptive metadata? • Has your organisation defined a minimum set of required fields in the metadata scheme to be filled out for each collection/digital object? • Is your organisation aware of domain specific information for each collection that should be considered in the descriptive metadata?

9.4. Preservation Procedure Policy: Metadata: Preservation metadata	
Related Guidance Policy	Metadata
Definition/Description	<p>DPC Tech Watch p. 5 describes preservation metadata as: “Metadata that supports the process of long-term digital preservation”.</p> <p>The organisation should create a policy that documents what relevant information about the preservation process is to be preserved and what additional information about the preservation process is required to be kept/documentated. This kind of metadata could also include metadata about rights and restrictions associated with the digital object or technical metadata.</p> <p>When preserving digital material at libraries, web archives or data centers PREMIS can be a useful metadata standard.</p> <p>The PREMIS Data Dictionary defines preservation metadata as:</p> <ul style="list-style-type: none"> • <i>“Supports the viability, renderability, understandability, authenticity, and identity of digital objects in a preservation context;</i> • <i>Represents the information most preservation repositories need to know to preserve digital materials over the long-term;</i> • <i>Emphasizes “implementable metadata”: rigorously defined, supported by guidelines for creation, management, and use, and oriented toward automated workflows; and</i> • <i>Embodies technical neutrality: no assumptions made about preservation technologies, strategies, metadata storage and management, etc.”</i>
Why	Preservation metadata is needed to be able to understand the digital material in the long term.
Risks	Not creating and preserving preservation metadata will endanger the understandability of the digital material.
Life cycle stage	Description Information & Representation Information, Preservation Planning, Create or receive; Ingest; Preservation Action; Store; Transform
Stakeholder	<p>Management: defines metadata policies and the use of standards</p> <p>Technology Manager: responsible for ensuring the proper systems for rendering the metadata and the digital material</p> <p>Consumer: needs to be able to access and trust the metadata in order to understand the digital material</p>
Cross Reference	Authenticity Standards Rights
Examples	<u>Yale University Library</u> : “ <i>Metadata is fundamental to preserving Yale University Library's digital resources. Preservation metadata includes a number of different types</i>

	<p><i>of metadata: <u>administrative</u> (used in managing information resources including rights and permissions), <u>technical</u> (describing hardware and software needed to maintain an information object) and <u>structural</u> (identifying the relationships between objects such as part of, dependent upon that form intellectual entities.” Source: http://www.library.yale.edu/iac/DPC/revpolicy2-19-07.pdf</i></p>
Control Policy	<ul style="list-style-type: none"> • All preservation events MUST be recorded • Information on preservation events SHOULD use the PREMIS schema • Information on preservation event MUST include date undertaken, action and agent
Questions to foster discussions	<ul style="list-style-type: none"> • Does your organisation use a formal standard for preservation metadata? • Has your organisation documented what information about the preservation process is to be preserved and what additional information about the preservation process is required to be created and preserved? • Does the metadata include information on the rights and restrictions associated with the digital collection?

9.5. Preservation Procedure Policy: Metadata: Structural metadata	
Related Guidance Policy	Metadata
Definition/Description	Structural metadata can be defined as metadata required to describe the internal structure and the component relationships of a digital object ² . Structural metadata contains information on how the digital object has been created, e.g. metadata collected when digitizing a book. The organisation should document relevant information about the ‘containers’ of the files in the structural metadata and decide what information is to be preserved and if a formal standard is to be used in preserving this type of metadata, for example: use of the METS standard.
Why	Structural metadata is important to be able to render the digital object authentically in the future.
Risks	Correctly rendering of the digital object may be lost if structural metadata is missing.
Life cycle stage	Description & Representation Information, Preservation Planning, Create or Receive, Ingest, Preservation Action, Transform
Stakeholder	Management: defines metadata policies and the use of standards Technology Manager: responsible for ensuring the proper systems for rendering the metadata and the digital material
Cross Reference	Bit Preservation Functional Preservation Access Authenticity Standards
Examples	State and University Library, Denmark: “Monitoring the international development in metadata standards includes descriptive, administrative (including technical) and structural metadata.” Source:, http://en.statsbiblioteket.dk/about-the-library/dpstrategi
Control Policy	<ul style="list-style-type: none"> Information on structure should be included The METS files SHOULD be able to be validated
Questions to foster discussions	<ul style="list-style-type: none"> Has the organisation decided on a metadata schema for structural metadata?

² DPC Tech Watch 13-03 p. 33

10.Guidance Policy: Rights

Introduction: Rights are an important factor in digital preservation. Rights issues are concerned with acquiring, preserving and making digital material accessible to the Designated Community. There is a variety of rights, for example Legal deposit, Archival deposit, Archival legislation, Privacy, Contract law, Copyright. National legislation and deposit/archiving agreements will have an impact on the rights of the digital material.

Policy Elements in this chapter

- 10.1 Comply with national legislation and contracts with business partners
- 10.2 Document Object creator /copyright holder
- 10.3 Enter into Deposit Agreements
- 10.4 Clarify legal context for preservation actions
- 10.5 Clarify rights related to specific types of material

10.1. Preservation Procedure Policy: Comply with national legislation and contracts with business partners	
Related Guidance Policy	Rights
Definition/Description	<p>An organization preserving digital collections should know and document what the national (archival) legislation applies to the holdings of the institution. If the institution should comply with any national legal deposit / national archival legislation scheme. This legislation often states both what kind of material is to be acquired and preserved, for how long, and who may access or require a copy of the archived material. The specific conditions stated in the legal deposit act / national archival legislation concerning the digital preservation and the access to and use of the digital material should be part of the policy for digital preservation in the institution.</p> <p>For information and data which can identify individuals extra security measures should be put in place. This might be data such as census returns or population studies, or it might be held within collections of private papers. This kind of information can be subject to legislation on personal data security.</p> <p>The organisation should ensure that the policy and access measures address the implications of unintended release and that the legislation that applies to personal data is considered in the policy.</p> <p>In some cases the organisation may enter into a contractual relationship with a third party in order to provide preservation services.</p> <p>The institution should make sure that the parts of the collection which the contract applies to are known and identified as such in the preservation framework.</p> <p>The organisation should ensure that the requirements in the contract are implemented in the digital preservation framework of the organisation.</p>
Why	The institution needs to obey the national legislation and any contracts with business partners in order to fulfil its mandatory obligations.
Risks	The institution risks law suits or security breaches if the institution does not obey the national legislation and business contracts.
Life cycle stage	Create or receive Ingest Access, use and reuse
Stakeholder	Management: needs to ensure that the organisation fulfil its legislative responsibilities Operational Management, Technical Management and System Architect need to implement the necessary measures
Cross Reference	Access Standards

	<p>Organisation Metadata</p>
Examples	<p>Cornell University Library “...define policies and procedures for the preservation and availability of digital assets respectful of intellectual property ownership and rights” Source: http://ecommons.library.cornell.edu/handle/1813/11230</p>
Control Policy	<p>For collection x</p> <ul style="list-style-type: none"> • Deposit agreement IS <value> • Geographic locations SHOULD be in EU • Number of copies of file >= 3
Questions to foster discussions	<ul style="list-style-type: none"> • Does any national legal deposit or archival deposit scheme apply to your organisation? • Does any of the information held have the information in it capable of identifying individuals? • Does your organisation have any contracts with external depositors of data?

10.2. Preservation Procedure Policy: Document Object creator /copyright holder	
Related Guidance Policy	Rights
Definition/ Description	<p>The organisation should make sure that information about the digital object creator / copyright holder is recorded in the administrative metadata in order to prevent future mistakes or uncertainty concerning rights.</p> <p>When the object creator is unknown the term orphan work is used. An orphan work is an object or collection where the object creator or copyright holder cannot be identified. This information should be in the administrative metadata in order to prevent future mistakes or uncertainty concerning rights. Examples of orphan works could be found in web archives or in old collections in libraries where the provenance of the digital object may be missing.</p>
Why	In order to be able to comply with copyright laws the organisation needs to keep track of digital object creator for all digital collections
Risks	If the organisation does not keep track of object creator it may violate copy right laws and risk law suits.
Life cycle stage	Description & Representation Information, Preservation Planning, Create or receive Ingest
Stakeholder	<p>Management: needs to ensure that the organisation fulfil its legislative responsibilities</p> <p>Operational Management, Technical Management and System Architect need to implement the necessary measures</p>
Cross Reference	Rights metadata
Examples	<p>Dartmouth College Library: <i>Intellectual Property: Dartmouth College Library is committed to providing access to digital materials while respecting and upholding the intellectual property rights of authors and obtaining prior consent when the creator's identity is known. Rights management actions will be documented and rights information will be preserved with digital content."</i></p> <p>Source:http://www.dartmouth.edu/~library/digital/about/policies/preservation.html?mswitch-redir=classic</p>
Control Policy	<ul style="list-style-type: none"> Original Metadata creator field SHOULD be completed
Questions to foster discussions	<ul style="list-style-type: none"> Is information about the digital object creator known and recorded in your repository? Does your organisation preserve orphan works?

10.3. Preservation Procedure Policy: Enter into deposit and archiving agreements	
Related Guidance Policy	Rights
Definition/Description	<p>For entire collections or part of collections the organisation might act on behalf of a depositor with whom there should be a deposit agreement. A deposit agreement or archiving agreement is a formal agreement between depositor of the collections and the organisation performing the preservation of the collections.</p> <p>A formal deposit agreement enables the depositor and the organisation to understand the roles and responsibilities for both parties. A deposit agreement can be general and cover all material deposited by the depositor or it can be collection specific and cover requirements concerning a specific collection or part of a collection. It can specify requirements such as retention period, action to be taken when migrating the material etc.</p> <p>The organisation could consider having a general deposit agreement to cover all types of material and collections, e.g. if the collections in the organisations are very homogenous. For general agreements the organisation should ensure that it covers special cases and that the requirements stated in the general deposit agreement are part of the policy for this collection. A general deposit agreement can clarify roles and responsibilities. If the organisation has collection or depositor specific deposit agreements the organisation should make sure that this information is implemented in the related policy.</p> <p>A deposit agreement should contain as a minimum information on:</p> <ul style="list-style-type: none"> whether the organisation is allowed to delete material at all or only under certain circumstances the organisation's policy for disposal that identifies the material to be deleted and under which circumstances the material can be deleted by the organisation the retention period for the material the measures needed to be in place to ensure that the deposit agreement is fulfilled whether the organisation is obliged to keep the original digital object, e.g. in case of migration or other kinds of preservation transformations. The information about keeping or disposing of the original in case of migration needs to be added to the information held about the digital object. access rights to the collection. <p>The organisation should ensure that all requirements regarding terms for preservation as stated in the deposit agreement are part of the policy for this collection.</p>
Why	A deposit agreement ensures that the digital material is preserved according to the requests of the depositor and that roles and responsibilities of both the depositor and the organisation are clear.

Risks	The lack of a deposit agreement can result in uncertainties about how to preserve a collection and poor decisions can thus be made.
Life cycle stage	Curate and Preserve, Create or receive, Ingest, Preservation Action, Access use and re-use, Transform, Dispose
Stakeholder	Management: needs to ensure that all agreements are fulfilled Depositor: needs to be assured that the organisation will fulfil all agreements
Cross Reference	Rights Metadata
Examples	National Library of Australia: <i>"Subject to collecting and preservation agreements that the Library may enter into from time to time with other agencies, the digital information resources for which we currently accept some level of preservation responsibility include (...)"</i> Source: http://www.nla.gov.au/policy-and-planning/digital-preservation-policy
Control Policy	For collection x <ul style="list-style-type: none"> • Deposit agreement IS <value> • Original object KEPT equal to YES • Geographic locations SHOULD be in EU • Number of copies of file >= 3 • File format MUST be <value> • Filechecksum-recalculation date <= today – 1 years
Questions to foster discussions	<ul style="list-style-type: none"> • Does your organisation have formal deposit agreements with the depositor of the collections? • Does your organisation have a general deposit agreement to cover all types of material and collections? • Does the deposit agreement give the right for the holding organisation to delete material? • Does the deposit agreement oblige the holding organisation to keep the original digital object, e.g. in case of migration or other kinds of preservation transformations? • Does the deposit agreement set a retention period for the digital objects being deposited? • Does the deposit agreement cover all types of material and collections?

10.4. Preservation Procedure Policy: Clarify legal context for preservation actions	
Related Guidance Policy	Rights
Definition/Description	<p>There may be requirements concerning the deposit of a collection with the organisation to ensure that preservation actions are undertaken within certain legal jurisdictions and this may limit the possible technical solutions. This could be the case with web archiving.</p> <p>The organisation needs to ensure that these requirements are part of the policy for this collection.</p>
Why	To be able to fulfil the terms agreed upon the organisation needs to be aware of all requirements.
Risks	If the requirements are not implemented in the policy for the collection poor decisions can be made.
Life cycle stage	Curate and Preserve, Create or receive, Ingest, Preservation Action, Access use and re-use, Transform, Dispose
Stakeholder	<p>Management: needs to ensure that all agreements are fulfilled</p> <p>Technology Management: needs to ensure that the technical set up can fulfil all legal obligations</p>
Cross Reference	<p>Access</p> <p>Authenticity</p> <p>Bit preservation</p> <p>Functional preservation</p>
Examples	<p>The Royal Library, Denmark: “Legislation regarding storage and access to these types of materials is more restrictive than for physical materials” Source: http://www.kb.dk/export/sites/kb_dk/da/kb/downloadfiler/PreservationPolicyDigitalMaterials_21092012.pdf</p>
Control Policy	<p>For collection x: Geographic locations SHOULD be in EU</p> <p>For collection z Geographic locations SHOULD be in EU or US</p>
Questions to foster discussions	<ul style="list-style-type: none"> • Do any of the collections have legal requirements for where preservation actions take place? • Do any of the collections have legal requirements for how the information is reproduced? • Do any of the collections have legal requirements for where the information

can be accessed?

11.Guidance Policy: Standards

"Standards cover a variety of topics and issues; they may be normative—setting requirements for quality and actions, or informative—describing and guiding the use of methods. In all cases they represent agreements that are generally, but not always, considered to be best practice. "(Source: [Aligning national approaches in Digital Preservation](#), 2012)

Whether the organisation applies external standards should be clear in the Policy. In this document the focus is on standards related to digital preservation, not on IT and Security.

For a good overview of relevant standards see the above mentioned document.

Many current policies of organisations not only describe that they want to adhere to standards, but they also are willing to participate in the creation of standards.

Policy Elements in this chapter

- 11.1 Principle on use of standards
- 11.2 Reference Model
- 11.3 Standards for various aspects of digital preservation

11.1. Preservation Procedure Policy: Principle on the use of standards	
Related Guidance Policy	Standards
Definition/Description	<i>"A standard is a specification of precise criteria designed to be used consistently and appropriately"</i> (Source: Aligning national approaches in Digital Preservation , 2012, which offers an extensive discussion of various aspects of standards), p. 115.
Why	As the digital collections will be taken care of by many different stakeholders over the years, it is important that each stakeholder can rely on the information in the collections and the standards that were used to create and manage it. Therefore the use of standards is highly applicable in digital preservation. A firm statement of the organisation on adherence to standards will add to the trustworthiness of the organisation.
Risks	The risk of not using standards are manifold: future generations might not understand the material and mistakes might be made
Life cycle stage	Curate and preserve, Preservation Planning (in principle this affects all stages in the life cycle)
Stakeholder	Management: need to set the overall approach to the use of standards Operational Management: need to implement standards in daily processes
Cross Reference	Metadata Access Bit Preservation Functional Preservation
Examples	Cornell University Library: <i>"CUL avows that the digital preservation program will:</i> <ul style="list-style-type: none"> <i>•comply with the Open Archival Information System (OAIS) reference model standard in the development of the digital archive</i> <i>•adhere to prevailing community -based standards in developing and maintaining its organisational and technological context</i> <i>•participate in the development of digital preservation standards and their promulgation"</i> Source: http://ecommons.library.cornell.edu/bitstream/1813/11230/1/cul-dp-framework.pdf
Control Policy	Some standards, such as the use of PREMIS for preservation metadata may apply to all parts of the collection, in other cases such as the use of a standard file format may only apply to specific subsets. Some examples of control policies relating to standards are: <ul style="list-style-type: none"> • Information on preservation events SHOULD use the PREMIS schema • Information on preservation event MUST include date undertaken, action and agent • The file checksum algorithm MUST be <name of algorithm>

<p>Questions to foster discussions</p>	<ul style="list-style-type: none"> • ISO standardized format equals YES • File format MUST be <value> • Format documentation is available equals YES <div> <ul style="list-style-type: none"> • Does your organisation use standards for digital preservation? • Is your organisation aware of all relevant national standards the organisation needs to adhere to? • Do your organisations have collections with specific relevant standards, for example standards in relation to file formats in a specific discipline? </div>
--	---

11.2. Preservation Procedure Policy: Reference Model	
Related Guidance Policy	Standards
Definition/Description	<p>A reference model can be defined as: <i>“A framework for understanding significant relationships among the entities of some environment, and for the development of consistent standards or specifications supporting that environment. A reference model is based on a small number of unifying concepts and may be used as a basis for education and explaining standards to a non-specialist.”</i> (Source: OAIS standard)</p> <p>The choice for a reference model for digital preservation is a fundamental one and will affect all the processes and procedures. The choices of various other standards is reflected in element 11.3 Use of specific standards</p>
Why	<p>When there is a commonly used standard in a particular domain, that is continuously being updated, it will benefit the organisation to adhere to this standard (both in costs, approaches, understandability, related training etc.) and be compliant with this standard reference model.</p> <p>The use of a standard reference model is a fundamental choice for a digital repository and should be included in the policy, as it guides various other aspects. The OAIS model, Open Archival Information System ISO 14721:2012 is generally seen as the standard reference model in digital preservation.</p>
Risks	Without standardisation the organisation might neglect important elements or not follow common principles. This might lead an isolated position for the organization and can be very expensive and risky.
Life cycle stage	Curate and Preserve
Stakeholder	<p>Management: the choice for a reference model will guide many of the activities in relation to Digital Preservation</p> <p>Operational Management, Technical Management and System Architect: need to implement the reference model</p> <p>Collection Management (non SHAMAN): support management from point of view related to the content to preserve</p>
Cross Reference	Bit Preservation Functional Preservation Metadata Access
Examples	<p>USCL : <i>“USC Libraries, with support from the University Technology Services, avows that the digital preservation program will:</i></p> <ul style="list-style-type: none"> <i>• comply with the Open Archival Information System (OAIS) reference model standard in the development of the digital preservation program where possible, such as with the MetaArchive Cooperative”</i> Source; <p>http://library.sc.edu/digital/USC_Libraries_Digital_Preserva.pdf</p>

Control Policy	This section is defining the approach to the creation and maintenance of the overall infrastructure and as such may not have control policies as control policies are concerned with the content and/or user community.
Questions to foster discussions	<ul style="list-style-type: none"> Does your organisation take a reference model as starting point for digital preservation?

11.3. Preservation Procedure Policy: Use of specific standards	
Related Guidance Policy	Standards
Definition/ Description	A lot of different standards for various aspects (e.g. Costs, File Formats, Metadata etc.) of Digital Preservation exist. Some are only applicable in a certain domain.
Why	When there is a commonly used standard in a particular domain, that is continuously updated, it will benefit the organisation to adhere to this standard (both in costs, approaches, understandability, related training etc.).
Risks	If an organisation has not implemented a standard that is commonly used in the domain, the organisation will risk an isolated position, and it might not be interoperable with similar organisations.
Life cycle stage	Curate and Preserve, Preservation Planning, Description and Representation Information
Stakeholder	<p>Depositor: might expect certain standards to be used in the organisation</p> <p>Consumer: might expect certain standards to be applicable in the data he will use from the repository</p> <p>Management: need to be aware of standards in use of their domain and the applicability for their organisation</p> <p>Operational Management, Technical Management and System Architect need to implement the agreed standards in the organisational processes</p>
Cross Reference	Metadata Digital Object Bit Preservation Functional Preservation Access
Examples	University of South Carolina Libraries: <i>"USC Libraries, with support from the University Technology Services, avows that the digital preservation program will: (...)</i> <ul style="list-style-type: none"> <i>• adhere to prevailing community-based standards in developing and maintaining its organisational and technological context"</i> Source:, http://library.sc.edu/digital/USC_Libraries_Digital_Preserva.pdf)
Control Policy	Some standards, such as the use of PREMIS for preservation metadata may apply to all parts of the collection, in other cases such as the use of a standard file format may only apply to specific subsets. Some examples of control policies relating to standards are: <ul style="list-style-type: none"> • Information on preservation events SHOULD use the PREMIS schema • Information on preservation event MUST include date undertaken, action and agent • The file checksum algorithm MUST be <name of algorithm> • ISO standardized format equals YES • File format MUST be <value> • Format documentation is available equals YES

Questions
to foster
discussions

- Has your organisation chosen a standard to describe preservation metadata for the digital objects in care?
- Has your organisation chosen a standard to refer to for describing the file formats in their repository?
- Has your organisation decided to comply with a file format standard? For example, if JPEG2000 is an agreed file format in the organisation for digitization activities, is it also described how close the published standard should be followed?
- Is it clear what the precise file format profile is, e.g. which parameters must be used to encode the files?
- Has your organisation decided on a standard for storage media?
- Has your organisation decided on a standard for data description?
- Has your organisation decided on following specific, may be discipline related, standards for record keeping and /or data management?
- How does your organisation handle the representation of contextual information and which are the standards to be followed in specific areas, like type of objects, agents (see for example the Premis Data Dictionary), time notation etc.
- Are there de facto standards not mentioned above that your organisation needs to follow?

12.Guidance policy: Access

As digital preservation is more than just storing information but also about making this information accessible and usable over time, organisations need to understand how their users will access the digital material. This could be as simple as taking into consideration how a digital object will be viewed but might also be expanded to include methods that enable User Communities (this can be a variety of Designated Communities) to reuse the digital material or engage with the digital content, or other computers harvesting material such as metadata. Several approaches can be chosen as they are not necessarily exclusive but may depend on the type of material. For example access to websites may use a different approach than data sets.

Policy elements in this chapter

- 12.1 Usability
- 12.2 Digital Rights Management
- 12.3 Design of Dissemination Information Package
- 12.4 Understandbilty for Designated Community
- 12.5 Search facilities/resource discovery
- 12.6 Designated Community identified

12.1. Preservation Procedure Policy: Usability	
Related Guidance Policy	Access
Definition/Description	<p>The organisation should describe how it wants to ensure the usability of the preserved digital collection.</p> <p>The organisation needs to know which rendering tools or environments offer the best “performance” for the digital object, performance is defined by the organization, for example “original look and feel” . In order to be able to do this, the organisation need to have a clear view on the characteristics (also called significant properties) of the digital objects.</p> <p>This knowledge is related to</p> <ul style="list-style-type: none"> the file format (s) of the digital object, the characteristics of the digital object the software/hardware needed to render the digital object and the identified designated community and their respective requirements. <p>Knowledge about file formats can be gained by identifying the digital objects in the collection. Not only the file format but also the environment is important for faithful rendering (for example the browser environment for websites) this knowledge is important to register as Representation Information.</p> <p>Knowing the file formats, the organization will need to investigate rendering tools, making decisions which ones to support and keep this knowledge up to date.</p> <p>Organisations might decide to offer the User Community the availability of dedicated (sometimes in-house) tools to best represent the digital material. The organisation could also rely on software in the User Community environment, but this should then be stated clearly and be adapted to changing habits. This information should be monitored regularly (Preservation Watch) as the requirements of the User Community can change over time.</p> <p>Risks in relation to access should be part of risk management procedures. The information about the risks can be derived from various sources, for example the access system will send error messages when users are unable to find the requested digital objects and the organisation need to have a process to deal with this.</p> <p>Related to the usability are availability times (for example 24*7) and accessibility restrictions (for example on site versus online), or material that is under embargo for a certain period of time</p>
Why	Digital preservation includes making the digital information accessible over time. As not only file formats but also rendering tools change over time, it is important that an organisation has a clear approach in safekeeping the environment in which the digital objects can be rendered faithfully.
Risks	<p>If no information is available about the rendering of the file format(s), the digital object might not be accessible for the intended users and the organisation will not meet its goals.</p> <p>As giving access to the preserved collection is a core functionality of the repository, all risks related to not being able to achieve these goals are endangering the continuity of the organisation</p>


Life cycle stage	Curate and Preserve, Community Watch and Participation Appraise and select, Preservation Action, Access, Use and Reuse, Description and Representation Information
Stakeholder	Consumer: needs to be informed Information Management: will realise the policies Collection Management (non Shaman): support management from point of view related to the content to preserve
Cross Reference	File format checks at Ingest Preservation Planning Metadata -> Representation Information Preservation Watch – Technology Watch to monitor the changes in the communities Designated Community
Examples	Boston University Libraries: <i>“The Libraries will take reasonable steps to ensure the usability of the digital objects.”</i> Source: http://www.bu.edu/dioa/openbu/boston-university-libraries-digital-preservation-policy/
Control Policy	Once the significant properties and access conditions have been established, these can form the basis of control policies. An example for a collection of MPEG2 files, the following control policies might set some of the significant properties and access conditions: <ul style="list-style-type: none"> • File format MUST be MPEG2 • The height of the video track >= 586 • Image width of the video >= 720 • Video bitrate >= 6000 • Number of tools available to render the file >= 3 • Number of free tools available >=2 • Format MUST have no license costs Whereas an example for a collection of digitized newspapers might include: <ul style="list-style-type: none"> • Colour model preserved MUST be TRUE • Compression type MUST be NONE
Questions to foster discussions	<ul style="list-style-type: none"> • Does your organisation need information about the “environment” to perform the digital object? • Does your organisation want to offer the user information about the “best environment”? • Does your organisation want to offer the user the tools to access the digital objects? • Does your organisation want to support different environments in their user groups? • Does your organisation want to offer only tools that support all the characteristics of the digital object?

12.2. Preservation Procedure Policy: Digital Rights Management (DRM)	
Related Guidance Policy	Access
Definition/Description	<p>Digital Rights Management can be defined as a set of technologies that are used with the intent to control the access and use of digital content and devices (via APARSEN WP31, source http://en.wikipedia.org/wiki/Digital_rights_management)</p> <p><u>PREMIS</u> mentions “inhibitors”: Features of the object intended to inhibit access, use, or migration.</p> <p><u>OAIS</u> page 1-8: “Access Rights Information: The information that identifies the access restrictions pertaining to the Content Information, including the legal framework, licensing terms, and access control. It contains the access and distribution conditions stated within the Submission Agreement, related to both preservation (by the OAIS) and final usage (by the Consumer). It also includes the specifications for the application of rights enforcement measures.”</p> <p>When applicable access to the digital collections should be in line with higher level access policies of the organisation as an organisation might have general access rules for their collections that need to be followed.</p>
Why	<p>Access to digital information can be restricted by digital rights. This can be incorporated in the digital object itself (for example by passwords) or as a general agreement with the producer of a collection or related to (inter-) national laws. Over the years, the digital rights will need to be enforced in a changing environment. This might influence the digital rights and the reputation of the organisation It is therefore important that an organisation has a policy in which it is describe which rights are relevant and how the organisation intend to deal with them.</p> <p>More on this at Rights; Deposit Agreement</p> <p>Access rights could be applicable for part of the User Community (for example only users that have Library membership will have access to a certain collection) or for specific collections.</p> <p>The management of the digital rights can take place in a separate system. Some digital right information can be added to the digital object via metadata.</p>
Risks	Lack of a policy might lead to infringement of rights of 3 rd parties and could also enable inappropriate or too restricted access
Life cycle stage	Community Watch and Participation, Preservation Planning, Appraisal and select, Access, use and reuse
Stakeholder	<p>Producer/depositor: need to give information about DRM and give input for policy</p> <p>Consumer: see Designated Community</p> <p>Management: will create DRM policy in line with organisational goals</p>
Cross Reference Examples	<p>Metadata -> rights</p> <p>Rights</p> <p>Yale University Library Policy: “Access:</p> <p><i>In preserving the accessibility of digital resources, the Library will:</i></p> <p><i>o Maintain information regarding rights and permissions governing access. “</i></p>

Control Policy	Source: http://www.library.yale.edu/iac/DPC/revpolicy2-19-07.pdf Digital Rights Management is likely to be enforced by the digital object management system, and although it will be codified, it is unlikely to be used in control policies for planning and watch activities.
Questions to foster discussions	<ul style="list-style-type: none"> • Has your organisation identified digital rights for a specific user community, for example students, elderly users, commercial users etc. • Has your organisation identified digital rights for a specific collection? • Has your organisation identified any geographic restrictions that might have implications for giving access to your collection?

12.3. Preservation Procedure Policy: Design of Dissemination Information Package	
Related Guidance Policy	Access
Definition/Description	<p>According to the OAIS model page 1-11 a Dissemination Information Package (DIP) can be defined as “an Information Package, derived from one or more Archival Information Packages AIPs, received by the Consumer in response to a request to the OAIS”.</p> <p>The needs of the various Designated Communities or Consumers related to usability will differ and it is important that the organisation develops a policy in which their approach to this variety is reflected. The usability for the Consumers can be highly dependent on the way the material is presented: some Consumers will be satisfied with a contemporary presentation of one digital object; others might best be served by a range of digital objects (separate website versus web collection). This is also related to the question whether the original version or a derived version will be presented (also referred to as “manifestations”.</p> <p>Related to this is the question of how long the organisation will guarantee that the material is accessible.</p> <p>If an organisation intends to meet the requirements of the user community applicable Dissemination Information Packages might need to be developed. The defined policy might also influence future preservation actions.</p>
Why	For a Consumer it should be clear what to expect from the collections in the repository in relation to the presentation of the digital collection.
Risks	The “usability” of the digital information is very dependent on the way the information is presented to the Consumers. If they are not satisfied the organization might lose its value to the community.
Life cycle stage	Preservation Planning, Community Watch and Participation, Access, Use and Reuse
Cross Reference	Designated Community
Stakeholder	Management: responsible for the Designated Community Collection Management (non Shaman): support management from point of view related to the content to preserve
Examples	<p>University of South Carolina Libraries: “Access to preserved digital content is provided using the most up to date technology available at the time of use. When retaining the look and feel is deemed necessary, USC will seek to enable the original versions of the digital objects to be rendered over time.” Source: http://library.sc.edu/digital/USC_Libraries_Digital_Preserva.pdf</p>
Control Policy	The design of the DIP is undertaken at the start of the infrastructure creation process and is unlikely to generate control policies, unless it is specific ones relating to validation at the ingest stage.
Questions to foster	<ul style="list-style-type: none"> Does your organisation have described how the digital object should be presented to the user community?

discussions	<ul style="list-style-type: none">• Does your organisation have described for how long they will present their digital objects to the user community?• Does your organisation want to develop different DIPs for different audiences?

12.4. Preservation Procedure Policy: Understandable for Designated Community	
Related Guidance Policy	Access
Definition/Description	The OAIS model page 1-12 defines “Independently Understandable” as a characteristic of information that is sufficiently complete to allow it to be interpreted, understood and used by the Designated Community without having to resort to special resources not widely available, including named individuals.
Why	As the digital objects will be preserved for the long term, explanation needs to be added to keep the information in the digital object understandable for future users. What type of information needs to be added to the digital object depends on the type of material. Sometimes it will be enough to refer to specific metadata, other times more “representation information” will be needed (for example to explain the meaning of rows and columns in a spread sheet). It is important that an organisation develops a preservation policy that describes the intended actions the organization should take to achieve the independent understandability for its users.
Risks	If the Designated Community does not fully understand the content and context of the digital objects, the information might be wrongly interpreted or not understood at all.
Life cycle stage Stakeholder	Community Watch and Participation, Preservation Planning, Appraisal and select, Ingest Producer/Depositor: need to add information that supports the understanding of the information provided by the digital object Management: responsible for the Designated Community Collection Management (non Shaman): support management from point of view related to the content to preserve
Cross Reference Examples	Designated Community University of Utah, J. Willard Marriott Library: <i>“The Library will strive to: Comply with OAIS and other digital preservation standards and practices Ensure that content remains readable and understandable”</i> Source: <i>Digital Preservation Policy (2012)</i> http://www.lib.utah.edu/collections/digital/DigitalPreservationPolicy2012.docx 
Control Policy	It can be difficult to ascertain whether the content is understandable by the designated community, but proxy measures can be used, for example: <ul style="list-style-type: none"> • Number of tools available ≥ 3 • Adoption of the file format is Good • Format Documentation is available
Questions to foster discussions	<ul style="list-style-type: none"> • Is your organisation willing and has the resources to add information so that the digital object is fully understandable for the user community? • Has your organisation developed procedures to check whether the digital

	information is still “independently understandable” for the user community?

12.5. Preservation Procedure Policy: Search facilities / resource discovery	
Related Guidance Policy	Access
Definition/Description	According to the OAIS model page 1-11 the terminology used is “Finding Aid” and defined as “a type of Access Aid that allows a user to search for and identify Archival Information Packages of interest”.
Why	<p>The organisation should consider how Consumers might want to find the information in the repository. This is important as it will affect the design of, for example, indexes to support the search for unique identifiers, but also because it could either limit or support the needs of the Consumers.</p> <p>Descriptive metadata, the use of Persistent Identifiers or local or domain specific identifiers will be important. If digital objects already have a persistent identifier before they enter the repository, it might be important to make the digital object accessible via this identifier.</p>
Risks	Not having a clear policy of how to make the digital information accessible, could lead to little or no use of digital collections in the repository
Life cycle stage	Description & Representation Information, Community Watch and participation, Access, Use and Reuse
Stakeholder	<p>Management: responsible for the Designated Community</p> <p>Collection Management (non SHAMAN): support management from point of view related to the content to preserve</p>
Cross Reference	Metadata
Examples	<p>Yale University Library Preservation Policy: “Access: <i>In preserving the accessibility of digital resources, the Library will: (...)Maintain the ability to locate the digital resource reliably.</i>”</p> <p>Source: http://www.library.yale.edu/iac/DPC/revpolicy2-19-07.pdf</p>
Control Policy	<p>Examples might include:</p> <ul style="list-style-type: none"> • Tools supporting access ≥ 1 • Descriptive metadata MUST comply with minimum set of fields • All objects SHOULD have a persistent identifier
Questions to foster discussions	<ul style="list-style-type: none"> • Does your organisation offer proper search facilities to the user community? • Does your organisation provide sufficient metadata to enable the user to find what he is looking for? • Does your organisation use persistent identifiers for all objects?

12.6. Preservation Procedure Policy: Designated Community/Communities identified	
Related Guidance Policy	Access
Definition/Description	The OAIS model page 1-11 defines “Designated Community” as “An identified group of potential Consumers who should be able to understand a particular set of information. The Designated Community may be composed of multiple user communities. A Designated Community is defined by the archive and this definition may change over time.”
Why	Knowing the Designated Community is important in order to serve them optimally and make the preserved information useable and understandable, which is a goal of preservation. There can be different users of the repository and the potential Consumers do not necessarily need to be outside the organisation but could also consist of staff or related institutions. The Designated Community might even differ per collection and should in this case be defined per Collection
Risks	If the organization as owner of the repository fails in identifying accurately the user community for a collection the intended User Community might not be able to understand, use or reuse the digital information in the repository. This could in time pose a serious risk to the survival of the collection.
Life cycle stage	Community Watch and Participation, Appraisal and select Access, Use and Reuse
Stakeholder	<p>Producer/depositor: will be able to tell who is the intended audience for this collection, for example researchers using a certain data set</p> <p>Management: will be able to tell the intended Designated Community of the collections in the repository</p> <p>Collection Management (non Shaman): support management from point of view related to the content to preserve</p>
Cross Reference Examples	<p>Dissemination Information Package</p> <p>Yale University Library Preservation Policy: <i>“This Policy recognizes that the <u>maintenance</u> and the reliable long-term access to Yale’s digital resources are supported by a preservation planning function. Research (monitoring) about technology that supports a repository and the requirements of the designated community it serves is a core activity to preservation planning, as well as outreach and education regarding policies, procedures and best practices for digital resources.”</i> Source: http://www.library.yale.edu/iac/DPC/revpolicy2-19-07.pdf</p> <p>Inter-university Consortium for Political and Social Research : <i>“The designated community at ICPSR, as described by OAIS, includes traditional users, i.e., social science researchers and graduate students at member institutions; and newer categories of users, e.g., undergraduates, policymakers, practitioners, and journalists.”</i> Source: http://www.icpsr.umich.edu/icpsrweb/content/datamanagement/</p>

	preservation/policies/dpp-framework.html
Control Policy	<p>In preparation for creating control policies, the organisation may identify the possible user communities/roles</p> <p>This could be very specific or at a minimum can relate to one of three roles: creator; manager/curator and end user.</p>
Questions to foster discussions	<ul style="list-style-type: none"> • Has your organisation identified the specific user group for specific collections? • Has your organisation described for all collections how they will be kept accessible to the user community?

13.Guidance Policy: Organisation

Digital preservation is not an isolated activity in an organisation, but requires involvement of several departments, each with its own responsibilities. These responsibilities should be reflected in the processes, the staffing, the budgets and the goals of the organisation as a whole. In the preservation procedure policies the organisation will describe in more detail how the organisation intends to achieve the defined preservation goals.

Policy Elements in this chapter

- 13.1 Staffing
- 13.2 Risk Management
- 13.3 Budgets
- 13.4 Preservation cost assessment
- 13.5 Roles and Responsibilities
- 13.6 Preservation goals

13.1. Preservation Procedure Policy: Staffing	
Related Guidance Policy	Organisation
Definition/ Description	An organisation that undertakes the long term preservation of digital collections will need dedicated and qualified staff, either in-house or contracted, to handle this.
Why	<p>The goals the organisation wants to achieve with respect to the long term accessibility of the digital collections can only be achieved if the digital material is handled by staff who have the professional skills and are aware of the risks. While digital preservation has long been an area of research, there is now consensus about the basic set of expertise that is needed and training programs and allocated budgets can help here. Explicit mentioning of the level of expertise the staff needs to possess is part of the policy. Regular updates should be part of a training plan, or Career Development Plan, as the knowledge may become outdated quickly.</p> <p>Staff are not restricted to IT staff, but must be seen in a broader sense, as all staff involved in the processes related to digital preservation, from the people that do the acquisition or creation (digitisation) of the material to the people involved in Ingest and Access.</p>
Risks	Inadequate staffing can pose a risk to the preservation of the digital collections as it might lead to poor decision making leading to damages to the collections in the repository.
Life cycle stage	Description and Representation Information, Preservation Planning, Community Watch and Participation, Curate and Preserve (as staff will be involved in all life cycles, the main Full Life cycle functions are mentioned here.
Stakeholder	Management: All management levels have a responsibility in appointing staff with adequate expertise
Cross Reference	Bit Preservation Functional Preservation
Examples	Yale University Library “ <i>The support of large scale storage is complicated and requires major investments in technology and staff</i> ” Source: http://www.library.yale.edu/iac/DPC/revpolicy2-19-07.pdf
Control Policy	<p>Staffing</p> <ul style="list-style-type: none"> • Running personnel costs MUST be less than 1M • Staff MUST be qualified on <value> scheme • Minimum Staff training MUST be 30 hours
Questions to foster discussions	<ul style="list-style-type: none"> • Does your organisation have a staffing strategy/plan for those responsible for preservation? • Has your organisation formulated the requirements for the resources/ staff involved in preservation (staff level of knowledge)? • Does your organisation have regular staff training plans and associated budget? • Does your organisation have resourcing levels sufficient to meet the stated

	<p>preservation goals?</p>
--	----------------------------

13.2. Preservation Procedure Policy: Risk Management	
Related Guidance Policy	Organisation
Definition/Description	Risk management is defined as: “Coordinated activities to direct and control an organisation with regard to risk.” (ISO/IEC Guide 73:2002, via Drambora Glossary)
Why	<p>Digital preservation is all about identifying and mitigating risks. Digital material is dependent on a technical environment. Risks are related to every aspect of handling these digital collections. It is important that an organisation has a process implemented to create a regular updated overview of the risks for the preserved collections and will act upon the risks identified with appropriate staff and procedures.</p> <p>The organisation needs to be confident that risks to all parts of the collection have been considered and appropriate mitigation measures have been taken. This is not to imply that all parts of the collection/collections should be treated equally, more that the risks to the collection should be understood and prioritised in line with the importance of the collection and available resources.</p>
Risks	If an organisation is not aware of the risks, it might lead to damage or even loss of collections and hence to loss of reputation, and the organisational goals will not be achieved. This could be a threat for the continuity of the organisation.
Life cycle stage	Curate and Preserve, Preservation Planning
Stakeholder	<p>Management: need to decide on risk management</p> <p>Operational Management: need to implement risk procedures and monitor the execution of it by operational management</p>
Cross Reference	<p>Standards</p> <p>Trustworthy Digital Repository</p> <p>Digital Object</p>
Examples	State and University Library, Denmark: “ <i>Digital preservation at the State and University Library is based on the principles of risk management. The library continuously manages and updates its digital preservation risk analysis in accordance with existing legislation and international standards.</i> ” Source:, http://en.statsbiblioteket.dk/about-the-library/dpstrategi
Control Policy	<p>Where the mitigating action for a particular risk is to watch for changes in the environment, it should be possible to monitor this. Examples of this are</p> <ul style="list-style-type: none"> • FormatShouldBeInternationalStandard SHOULD be Yes • Number of tools available >= 1
Questions to foster discussions	<ul style="list-style-type: none"> • Has your organisation done risk assessments on all collections in its care? • Are there procedures implemented related to risk management of the preserved collections? • Are the IT activities involved in the risk management procedures?

13.3. Preservation Procedure Policy: Budgets	
Related Guidance Policy	Organisation
Definition/Description	Preservation of digital collections is cost-intensive and it is important that budgets are in line with the preservation goals of the organisation.
Why	An organisation needs to be aware of the available budget in relation to the goals and commitments made with respect to preservation of digital collections. The organisation need to consider priorities within the wider funding envelope and using a cost model related to digital preservation may support this. The 4C project in the draft report " Evaluation of Cost Models & Needs " defines a cost model as "a representation of the resources, such as capital and labour, used for digital curation activities." The identification of clear priorities is vital to ensure that any budget fluctuations can be managed successfully.
Risks	If the budget is insufficient, the organisation might not be able to achieve their goals or commitments, which might lead to inability to perform committed tasks, take necessary actions and eventually cause loss or damage to the collections and ultimately to the organisation itself.
Life cycle stage	Description and Representation Information, Preservation Planning, Community Watch and Participation, Curate and Preserve
Stakeholder	Management: will allocate budgets
Cross Reference Examples	Costs Wellcome Library Preservation Policy: " <i>The Library allocates a proportion of its annual budget to support activities to ensure that the preservation policy can be implemented.</i> " Source: http://wellcomelibrary.org/content/documents/policy-documents/preservation-policy
Related Control Policy	Monitoring whether changes in costs might influence the budget available is one possibility. For plans involving actions, there are usually budgetary limits. Examples might be: <ul style="list-style-type: none"> • Running costs per object MUST be less than 0.24 • Action objective = cost less than 10.000 euro • Quantitative archival storage costs MUST be less than 0.34 • Personnel costs MUST be less than 1M
Questions to foster discussions	<ul style="list-style-type: none"> • Does your organisation have a financial plan for the repository/collection to ensure sufficient resources are available for running the repository?

13.4. Preservation Procedure Policy: Preservation Cost Assessment	
Related Guidance Policy	Organisation
Definition/Description	Preservation cost assessment is the identification of all costs related to digital preservation of the collections under care.
Why	In order to be able to allocate real life budgets it is important that an organisation knows the costs of different aspects of digital preservation. The policy will describe how the organisation plans to get an overview of the costs in relation to the digital preservation activities.
Risks	Although the costs of various preservation activities are directly related to each organisation's infrastructure, it is important to know the costs of preservation activities in order to plan for budgets and act within the boundaries of the availability of the budget.
Life cycle stage	Description and Representation Information, Preservation Planning, Community Watch and Participation, Curate and Preserve
Stakeholder	Management: (Financial) will assign and monitor costs versus budgets
Cross Reference Examples	Budget National Library of New Zealand: <i>"Successful digital preservation demands that: Solutions for preserving digital materials must be cost-effective and can be resourced as business-as-usual"</i> Source; http://archives.govt.nz/sites/default/files/Digital_Preservation_Strategy.pdf
Control Policy	In order to create adequate control policies in relation to costs it is important to have: <ul style="list-style-type: none"> • Available budgets for preservation actions • Budgets available in near future An example might be: <ul style="list-style-type: none"> • Running costs per object MUST be less than 0.24
Questions to foster discussions	<ul style="list-style-type: none"> • Is your organisation aware of the costs of each step in the preservation lifecycle? • Has your organisation undertaken a cost/benefit analysis to ensure that the policies and procedures are cost-effective?

13.5. Preservation Procedure Policy: Roles and Responsibilities	
Related Guidance Policy	Organisation
Definition/Description	Roles and responsibilities with regard to the preservation of the digital collections should be clear to the employees in the organisation and written down in processes and procedures that are regularly updated.
Why	It is important that everyone in the organisation is aware of who is responsible for what. During the lifecycle of the digital collections various decisions need to be taken and actions planned from deciding which collections will be created, the criteria under which collections will be accepted, the quality control measures and the approval of preservation plans. It is important for achieving the digital preservation goals that the organisation has a clear view who is involved and who is entitled to make decisions. In some cases collections might have owners that are outside the organisation and it is important to identify the responsibilities in these cases. Deposit agreements and contracts should make this clear.
Risks	Lack of understanding roles and responsibilities might lead to misunderstandings, ad hoc solutions, and decisions that are not in line with the organisational policies. Ultimately it can lead to loss of trust.
Life cycle stage	Description and Representation Information, Preservation Planning, Community Watch and Participation, Curate and Preserve
Stakeholder	Management: on all levels management should be involved in defining roles and responsibilities
Cross Reference Examples	<p>Staffing and expertise</p> <p>Portico where all stages have an appointed role that is responsible for making decisions about for example deletion of content, change of tools, collection building and preservation actions Source: Portico, http://www.portico.org/digital-preservation/wp-content/uploads/2011/03/Portico-roles-responsibilities.pdf</p> <p>UK Archaeology Data Service: which defines the preservation responsibilities and activities for the following roles: Director, Collections Manager, Systems Manager, User Services Manager, Administrator, Application developer, Curatorial staff and finally all staff. See policy for details. Source: http://archaeologydataservice.ac.uk/attach/preservation/PreservationPolicyV1-1.pdf</p>
Control Policy	<p>The stakeholders and roles used in the control policies for automated use need to map to the appropriate stakeholders in the organisation.</p> <p>In addition, any tools being used need to have the right stakeholder set up to receive information about events and plans and make any decisions.</p>

Questions
to foster
discussions

- Does your organisation have defined a policy that indicates which are the roles for those departments and personnel involved in preservation?
- Does the repository hold any agreements or contracts that discuss responsibilities of partners?

14.Guidance policy: Audit and Certification

There is general consensus in the Digital Preservation community that audit and certification is welcome and there are many organisations who expressed in their policies the intention that they want to be certified within the next few years. For audit and certification in Europe there is the European Framework for Audit and Certification, which starts with obtaining the Data Seal of Approval (basic), then do a self-audit against the ISO 16363 (extended) and if everything is compliant with the standard, then go for the external audit of ISO 16363 or DIN 31644 (full).

In this chapter the elements are related to the organizational intention to be audited and certified. However, the audit will concern the current practice of an organisation and is related to the processes and activities the organisation will develop in order to preserve the digital collections in a professional way. As such the policies related to audit and certification will not require specific policies, as the aim to get audited are not likely to lead to implementation of new processes.

Policy Elements in this chapter

- 14.1 Standard for Audit and Certification
- 14.2 Audit Preparations

14.1. Preservation Procedure Policy: Standard for Audit and certification	
Related Guidance Policy	Audit and Certification
Definition/Description	An audit might lead to a certification of a digital repository if the repository meets the qualifications.
Why	<p>If an organisation has the explicit wish, or is forced to be by funders, for example, to undergo an audit, it is important to mention which standards for Audit and Certification are applicable. Currently the main standards are</p> <ul style="list-style-type: none"> - Data Seal of Approval - DIN 31644 - ISO 16363 <p>The European Framework for Audit and Certification describes three levels: from basic to full certification.</p>
Risks	If the level of Audit and Certification is not mentioned, the funding bodies and the public might be misled
Life cycle stage	Curate and Preserve
Stakeholder	<p>Management: decides whether an audit and certification will take place</p> <p>Auditor: responsible for the audit process</p>
Cross Reference Examples	<p>Standards</p> <p>National Library of Australia: <i>“In developing or adopting relevant systems and infrastructure, the Library aims to operate within the principles of reliable digital repositories as defined by international standards and best practices(…)”</i> Source:, http://www.nla.gov.au/policy-and-planning/digital-preservation-policy</p> <p>John Hopkins University Libraries: <i>“The Sheridan Libraries Library Digital Program and the Sheridan Libraries Systems Department are responsible for repository audits. The repository audit establishes confidence in the authenticity and completeness of digital content. All managed activities will be documented according to evolving standards so as to provide an audit trail which meets criteria as described in the Implementation Plan required by projects such as The Center for Research Libraries Trustworthy Repositories Audit and Certification (TRAC)”</i> Source: http://old.library.jhu.edu/collections/institutionalrepository/irpreservationpolicy.html</p>
Control Policy	To be able to achieve this objective, the control policies will be described in the sections relating to the specific activity, there isn't anything specific to Audit and Certification per se.
Questions to foster discussions	<ul style="list-style-type: none"> • Has your organisation decided whether to be certified or not? • Has your organisation decided on a standard to use in the certification process? • What is the main reason to be audited/certified? • Are all staff members involved in digital preservation aware of the consequences of

	being audited?

14.2. Preservation Procedure Policy: Audit preparations	
Related Guidance Policy	Audit and Certification
Definition/ Description	Several issues need to be clarified in the policies with relation to the audit. Which level of audit is an organization aiming for and which time line does an organization have in mind. An audit does not necessarily be related to all collections in an organization but might be focused on a specific part, for example only the objects that will be preserved for the long term, or to a specific collection, for example the web archive of an organisation. These aspects are also important for budgeting and planning purposes
Why	It is important to make a general intention to be audited and to get certified more explicitly, for example make clear which part of the collections will be involved in an audit process and which collections are excluded
Risks	Not following up the guidance policy of becoming audited and eventually certified, might lead to loss of trust in the organization
Life cycle stage	Preservation Planning
Stakeholder	Management: will decide which collections will be in scope of an audit Auditor: responsible for the audit process
Cross Reference	
Examples	
Control Policy	To be able to achieve this objective, the control policies will be described in the sections relating to the specific activity, there isn't anything specific to Audit and Certification per se.
Questions to foster discussions	<ul style="list-style-type: none"> Is it clear to everyone involved in preserving digital material which activities will be part of an audit program? Is there a budget for audit planned and will the necessary staff be available?

15. Further Reading

- [1] Beagrie, N et al: Digital Preservation Policy Study, 2008
http://www.jisc.ac.uk/media/documents/programmes/preservation/jiscpolicy_p1finalreport.pdf
- [2] An overview of published preservation policies used for this Catalogue can be found at
<http://wiki.opf-labs.org/display/SP/Published+Preservation+Policies>
- [3] The National Archives: Digital Preservation Policies: Guidance for Archives, 2011
<http://www.nationalarchives.gov.uk/documents/information-management/digital-preservation-policies-guidance-draft-v4.2.pdf>

Authenticity

- [4] D24.1 Report on Authenticity and Plan for Interoperable Authenticity Evaluation System, APARSEN project, http://aparsen.digitalpreservation.eu/pub/Main/ApanWp24/APARSEN-REP-D24_1-01-2_4.pdf

Bit Preservation

- [5] E.M.Olmütz Zierau: A Holistic Approach to Bit Preservation. Thesis 2011, Hvidovre
- [6] Bit Preservation: A Solved Problem?" by David S. H. Rosenthal, International Journal of Digital Curation Vol 5, No 1, 2010 <http://www.ijdc.net/index.php/ijdc/article/view/151>)
- [7] NDSA levels of preservation: <http://www.digitalpreservation.gov/ndsa/activities/levels.html>
- [8] Persistent Identifiers Interoperability Framework, APARSEN project
<http://www.alliancepermanentaccess.org/wp-content/plugins/download-monitor/download.php?id=D22.1+Persistent+Identifiers+Interoperability+Framework>

Functional Preservation

- [9] The Parliamentary Archives Digital Preservation Policy,
<http://www.parliament.uk/documents/upload/digitalpreservationpolicy1.0.pdf>
- [10] Article on Danish website on Functional preservation, <http://digitalbevaring.dk/logisk-bevaring/>
(in Danish)
- [11] Definition of functional preservation: http://en.wikipedia.org/wiki/Digital_preservation
- [12] TRAC, http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf

Digital Object

- [13] <http://www.nationalarchives.gov.uk/documents/information-management/rm-code-guide8.pdf>
- Disposal policy of UK National Archives
- [14] Charlesworth A: Intellectual Property Rights and Preservation [PDF 1187KB] DPC Technology Watch
Report 12-02 <http://dx.doi.org/10.7207/twr12-02>:

Metadata

- [15] METS standard, <http://www.loc.gov/standards/mets/>
- [16] Metadata standards at DCC, <http://www.dcc.ac.uk/resources/metadata-standards>
- [17] Premis Data Dictionary version 2.1 www.loc.gov/standards/premis/v2/premis-2-0.pdf
- [18] DPC Tech Watch report <http://dx.doi.org/10.7207/twr13-03>
- [19] Article on metadata on Danish website <http://digitalbevaring.dk/metadata/> (in Danish)
- [20] Jenn Riley, Poster: www.dlib.indiana.edu/~jenrile/metadatamap/
- [21] Jenn Riley, Dictionary:
www.dlib.indiana.edu/~jenrile/metadatamap/seeingstandards_glossary_pamphlet.pdf

- [22] Gartner, Richard: Metadata for digital libraries: state of the art and future directions, JISC Technology & Standards Watch, version 1.0, April 2008,
http://www.jisc.ac.uk/media/documents/techwatch/tsw_0801pdf.pdf
- [23] Technology Watch Report 13-3: [Preservation Metadata \(2nd edition\) \[986KB\]](#) by Richard Gartner and Brian Lavoie (See also [First Edition, \(05-01 2005\)](#)). New DPC report
- [24] Significant properties:
<http://www.jisc.ac.uk/whatwedo/programmes/preservation/2008sigprops>
- [25] www.digitalbevaring.dk (in Danish)
- [26] ['Oh, you wanted us to preserve that?!' Statements of Preservation Intent for the National Library of Australia's Digital Collections.](#) Colin Webb, David Pearson, Paul Koerbin (National Library of Australia). D-Lib, vol 19, issue 1-2.
- [27] doi:10.1045/january2013-webb

Access

- [28] The APARSEN project has a work package related to Digital Rights Management (later update) and their results will be a good source.
- [29] The CASPAR project Report on OAIS Access Model
http://www.casparpreserves.eu/Members/cclrc/Deliverables/report-on-oais-access-model/at_download/file.pdf

Rights

- [30] See APARSEN project: D31.1 Report on DRM preservation (to be available soon)
- [31] For rights management metadata [ODRL](#) (Open Digital Rights Language) can be a useful standard,
<http://en.wikipedia.org/wiki/ODRL>.
- [32] For technical metadata e.g. the standard MIX (for images) could be used,
<http://www.loc.gov/standards/mix/>.
- [33] Farrell, T. ; Kim, Y. ; Pinsent, E. ; Kopidaki, S. ; Rynning, M. ; Manolopoulos, I. ; Papadopoulou, O. ; Arampatzis, S. ; Trochidis, I. ; Zioga, D: BlogForever D3.3: Development of the Digital Rights Management Policy, 2013 <https://zenodo.org/record/7518>

Standards

- [34] A good overview of standards currently in use can be found at " source: Aligning national approaches in Digital Preservation , 2012
http://educopia.org/sites/educopia.org/files/ANADP_Educopia_2012.pdf

Organisation

- [35] Staffing: The Digital Curator Vocational Education Europe Project DigCurV project <http://digcur-education.org/eng/Resources>
- [36] Costs: <http://www.4cproject.eu/>
- [37] Creating a business case for digital preservation is described in the DPC Business Case
http://wiki.dpconline.org/index.hp?title=Digital_Preservation_Business_Case_Toolkit
- [38] Risks Drambora information, see <http://www.repositoryaudit.eu/>

Audit and Certification

- [39] Audit and certification of trustworthy digital repositories ([ISO 16363](#))
- [40] Data Seal of Approval ([DSA](#))
- [41] Nestor Seal for Trustworthy Repositories based on DIN 31644 Criteria for trustworthy digital archives, [DIN 31644](#)
- [42] See the [website](#) of the Primary Trustworthy Digital Repository Authorisation Body (PTAB) where information can be found how to prepare for an audit