Collaboration to Clarify the Cost of Curation

D4.3—Quality and trustworthiness as economic determinants in digital curation

Deliverable Lead:	NLE
Related Work package:	WP4
Author(s):	Raivo Ruusalepp (NLE) Matthew Woollard (UKDA) Hervé L'Hours (UKDA) Lauri Leht (NLE) Diogo Proença (INESC-ID) Jaan Krupp (NLE) Neil Grindley (Jisc)
Dissemination level:	Public
Submission date:	14th March 2014
Project Acronym:	4C
Website:	http://4cproject.eu
Call:	FP7-ICT-2011-9
Project Number	600471
Instrument:	Coordination and support actions (CSA)—ERA-NET
Start date of Project:	01 Feb 2013
Duration:	24 months

Project funded by the European Commission within the Seventh Framework Programme		
Dissemination Level		
PU	Public	✓
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Version History

Version	Date	Changed pages / reason	Modified by
0.82	12th Mar 2014	Style edit	PLSS
1.00	14th Mar 2014	Released version	PLSS

Acknowledgements

This report has been developed within the project “Collaboration to Clarify the Cost of Curation” (4cproject.eu). The project is an ERA-NET co-funded by the 7th Framework Programme of the European Commission.

The 4C participants are:

Participant organisation name	Short Name	Country
Jisc	JISC	UK
Det Kongelige Bibliotek, Nationalbibliotek og Københavns Universitetsbibliotek	KBDK	DK
Instituto de Engenharia de Sistemas e Computadores, Investigacao e Desenvolvimento em Lisboa	INESC-ID	PT
Statens Arkiver	DNA	DK
Deutsche Nationalbibliothek	DNB	DE
University of Glasgow	HATII-DCC	UK
University of Essex	UESSEX	UK
Keep Solutions LDA	KEEPS	PT
Digital Preservation Coalition Limited by Guarantee	DPC	UK
Verein Zur Forderung Der It-Sicherheit In Osterreich	SBA	AT
The University of Edinburgh	UEDIN-DCC	UK
Koninklijke Nederlandse Akademie van Wetenschappen -Knaw	KNAW-DANS	NL
Eesti Rahvusraamatukogu	NLE	EE

Author(s): Raivo Ruusalepp (NLE), Matthew Woollard (UKDA), Hervé L’Hours (UKDA), Lauri Leht (NLE), Diogo Proença (INESC-ID), Jaan Krupp (NLE), Neil Grindley (Jisc)

Table of Contents

Figures

Tables

Executive Summary

This deliverable of the 4C project work package Enhancement is part of a suite of case studies into indirect economic determinants that were analysed in deliverable D4.1 *A prioritised assessment of the indirect economic determinants of digital curation*. This report discusses costs and benefits of standards-based quality assurance that is associated with trustworthiness through audits and certification practice.

The primary approach of applying standards to ensure quality in digital curation is at present focussed at the level of processes and operation. The evaluation of quality of digital archive processes, workflows, information security and quality of services is the object of self-assessment and formal audits. Quality and trustworthiness have become nearly synonymous in the digital curation discourse and merged into the practice of auditing trusted digital repositories.

At least five methods have been proposed to evaluate the trustworthiness of digital repositories, ranging from self-assessment (DRAMBORA, DSA) to formal audit and certification by external auditors (TRAC, DIN 31644, ISO 16363). These are used in two main ways: first, to increase the trustworthiness of the repository among its stakeholder groups and ultimately achieve a better reputation for the organisation; second, to increase the quality of processes being undertaken. Trustworthiness and reputation are seen as being enhanced through the publication (transparency) of audit results (which has become synonymous with assessment of quality).

As the concept of auditing is becoming part of the mainstream dialogue in digital repositories, the potential motivations for undertaking audits remain diverse. Most organisations undertaking audits will make a business case for undertaking the audit based upon a combination of these factors:

- to improve the work processes;
- to meet a contractual obligation;
- to provide a publicly understandable statement of quality and reliability.

The costs of quality assurance of processes have turned out to be hard to measure and benchmark because quality is determined directly or indirectly by multiple overlapping cost factors and costs are shared between many activities across longer periods of time. The data collection exercise of this task did not succeed in gathering audit and certification related cost data through a questionnaire because the required data was not readily available or could not be made public. As soon as these issues became fully apparent we reconsidered our methodology and focussed on a more qualitative approach. We carried out interviews with a series of senior digital repository managers, who were known to have carried out some form of audit and certification process and specialists within the digital curation domain. We also set up a focus group to discuss our preliminary findings in depth with our advisory board members representing funding organisations (with responsibility for data archives).

Our data collection and analysis made it clear that detailed costing is seldom part of the initial work on audit, and benefits begin to accrue already from simple exploration and preparation for addressing the audited issues. Many of the processes involved in audit—for example records management improvement, business process analysis—overlap with other desirable business outcomes and it is often impossible to identify such work as purely an investment for audit. The reports from the digital curation community testify that the primary motive for undergoing assessment or audit at this stage is pragmatic. Financial benefits through improved efficiency and quality of work are not the primary motives, partly because they are very difficult to ascertain among the total costs of the curation function.

1 Introduction

Digital curation is about ensuring that digital objects remain usable. Quality is a term that encompasses utility, objectivity, and integrity. In digital curation, quality assurance increases the chances of the digital objects being re-used over time. A trusted digital repository is one whose mission is to provide reliable, long-term access to managed digital resources to its designated community, now and in the future (RLG/OCLC 2002, p 5). Trust in a digital repository is related not only to trusting the preservation methods applied by the repository, but also to broad organisational issues like the funding base, policy framework, staff training, existence of transferable skills, and so on. A trustworthy digital repository will understand threats to and risks within its systems and organisation. Quality and trustworthiness have become nearly synonymous in the digital curation discourse and merged into the practice of auditing trusted digital repositories. This report examines the quality and trustworthiness issues from both a costs and a benefits point of view to clarify and elaborate the business case of auditing and certifying digital repositories.

1.1 Goals of the report

This report follows an early deliverable of the 4C project (D4.1—*A prioritised assessment of the indirect economic determinants of digital curation*) that discussed indirect economic determinants as generic management tools that can be applied in any organisation to help ensure sustainable digital curation. Among the 15 factors that were recommended by the 4C project stakeholders as indirect economic determinants trustworthiness was ranked second most important after risk. This report takes a closer look at the economic model of quality assurance in digital curation and aims to bring out the main cost factors as well as the benefits of standards-based quality assurance approach. Auditing is an example of standards-based quality assurance approach. The output from this task is to show how costing of digital curation can include consideration of trust, and that this is a significant gap in the existing cost models. The approach we have taken is to set the stage by providing an overview of the relationship between audit and certification, then to address the major benefits (and some of the issues) prior to talking about the costs.

The **target audience** of this report are senior repository managers and repository funders.

1.2 Scope of the report

The intended scope for this report was to be a case study report on the overhead, cost, intellectual input and the eventual benefits that may accrue of undergoing audit and certification procedures to become a ‘trusted digital repository’ or similar nomenclature. With this outcome in mind the report provides an initial outline of a method for calculating the costs and benefits of audit and certification (section 4). It also includes recommendations for the economic sustainability reference model (section 5.2). The analysis of available audit and certification cost data remains a work in progress for a number of reasons explained in detail in section 4.4 but primarily because the certification of repositories based on ISO 16363 *Audit and Certification of Trustworthy Digital Repositories* has not reached the level of implementation maturity which we expected it would have by the time this project and report were being developed. The International Organization for Standardization published ISO 16363 in February 2012. Publication of the corresponding draft ISO/DIS 16919 Requirements for Bodies Providing Audit and Certification of Candidate Trustworthy Digital Repositories, has been delayed whilst the Primary Trustworthy Digital Repository Authorisation Body (PTAB), which drafted ISO 16363 and ISO/DIS 16919, works with two ISO affiliated bodies, the ISO Committee for Conformity Assessment (CASCO) and the International Accreditation Forum (IAF), over their respective roles in the audit and certification process for Trustworthy

Digital Repositories. Until this discussion is concluded and the associated language in the draft ISO/DIS 16919 is completed and published, no audit against ISO 16363 can be conducted.

We have been able to collect and analyse various cost information which has allowed us to make a series of tentative conclusions about the state of the art in the assessment of the costs and benefits—as they apply to the audit and certification of digital repositories and digital curation activities—which should support some rich interactions with the conclusions of other 4C project tasks and work packages and provide valuable input into the roadmap work (WP5).

We have undertaken a series of interviews with senior digital repository staff, archivists, research funders (those with responsibility for data archives), and specialists within the digital curation domain that have confirmed some assumptions and informed our conclusions.

Digital repository audit checklists and, indeed, this report make several references to the RLG/OCLC *Trusted Digital Repositories: Attributes and Responsibilities* (2002). The length of time since this report was produced combined with its continued applicability helps indicate the journey repositories have taken before developing a small collection of nascent trust standards. The conclusion of this report reflects upon the maturity of these standards in the context of the slowly growing community support for using them in a rather short time of their existence. However, it should be noted that this report does not provide an assessment of the validity or usefulness of any audit process. It is clear that the relative costs and benefits of attaining TDR-status must be examined, independently from the assessment of the TDR-standards themselves, in order to ensure an independent and impartial assessment of the relationship between the costs and benefits of implementing and maintaining those standards.

1.3 Core terminology

For the purposes of this report we use certain terminology to define a generalised workflow around the whole of what is informally known as an audit process. These are discussed below (section 2.1). We also use the term ‘standard’ broadly to define assessment criteria; not all represent formally maintained standards. Note: Terminology can be expanded and the text aligned with the project’s common vocabulary.

Business case: an argument usually presented as a document to convince a decision maker to approve an action. The argument should justify the use of resources to support a business need. For this document the business need is carrying out some form of assessment (either a self-assessment, or a formal audit).

Internal Review: the process by which an organisation undertakes a review of the controls within a standard to develop a statement of applicability (defining which controls do, and do not apply, and thus either within or beyond the scope of the audit).

Preparation process: creating a statement of applicability listing all controls in the standard and listing the existing evidence to support each of the applicable controls in the standard.

Self-Assessment: an informal assessment of conformity by the organisation under observation. (The term self-audit is often used by organisations incorrectly). The results should provide a self-assessed statement of conformity to each ‘control’ thereby defining an overall level of conformance. A self-assessment may also result in a Corrective Action Plan whereby the organisation has a record of the actions that it would need to carry out in order to meet the requirements of the standard.

Audit: the formal assessment of conformity by independent parties. An audit may also result in a Corrective Action Plan whereby the organisation has a record of the actions that need to carry out in order to maintain the requirements of the standard.

Corrective Action: Operationalizing and implementing a Corrective Action Plan.

Certification: the assignment of a certificate to a body or system related to a standard. In the case of ISO certification, third parties offer these services. ISO does not offer certification though its committee on Conformity Assessment (CASCO) has produced a number of standards defining international consensus on voluntary criteria in certification good practice.

Post-audit surveillance: formal continuous assessment of conformity and improvement by independent parties, at scheduled times. Post-audit surveillance is generally a precondition of continued certification.

Each of these activities within the overall audit and certification process should be able to have a cost attached to them.

2 Introducing quality and trustworthiness of digital curation

Various standards exist for ensuring quality of processes and products in an organisation, ISO 9000 series of quality management system standards being the best known of these. Applying such standards provides an organisation with methods for controlling the quality of their operations, services and products. Using quality standards is often perceived as contributing towards a higher reputation for organisations.

Quality of operations, services and products have together become associated with the concept of 'trust' within the digital curation community and with the term trusted digital repository (TDR). The formal checking of the quality of operations may enhance the reputation of a repository but trust *per se* should be engendered through measurable standardised controls.

At the time (2002) when RLG and OCLC published their report *Trusted Digital Repositories: Attributes and Responsibilities*, digital preservation was perceived as a complex task that assumed highly skilled staff, access to costly computer infrastructure and interdisciplinary know-how. The TDR characteristics sought to define sustainable digital archives that could serve large-scale, heterogeneous digital collections held by national-level organisations with long-term digital preservation mandates. One of the qualities of the TDR was set as: "design its system(s) in accordance with commonly accepted conventions and standards to ensure the on-going management, access, and security of materials deposited within it" (TDR 2002). The ISO 16363 describes its quality metrics as (p. 10):

> *"Metrics are empirically derived and consistent measures of effectiveness. When evaluated together, metrics can be used to judge the overall suitability of a repository to be trusted to provide a preservation environment that is consistent with the goals of the OAIS. Separately, individual metrics or measures can be used to identify possible weaknesses or pending declines in repository functionality."*

Through this conjecture and compliance requirement with the OAIS reference model (that has since become standardised as ISO 14721:2003) quality of operations and services has become a component in the concept of a trustworthy digital archive. For some stakeholders a digital archive that can render digital objects in its care usable over a long period of time is already demonstrably providing a quality service and, hence, can be relied on to continue to do so. For other stakeholders the quality or efficiency of operations that can be certified against quality criteria through audit and certification are required to trust the repository.

In the digital preservation community trust has sometimes become an end in itself and a repository will strive to increase its reputation through certification. This report is based on the understanding that quality in all components of digital curation is a precondition of trustworthiness. Standards-based approaches to repository design, implementation and continuous improvement are formal and inculcate quality, if the results of applying standards are publicised or made available to stakeholders who are interested in trusting the organisation. The TDR auditing and certification practice is, thus, here viewed as one method of standards-based quality assurance.

2.1 Establishing trustworthiness

A central challenge of long-term digital preservation is the ability to guarantee the authenticity and understandability of digital objects across time. This is at risk due to different factors: ageing storage media, obsolescence of underlying systems and software, changes in technical and organisational infrastructures, as well as malicious or erroneous human actions. An organisation can be trusted to

successfully be responsible for long-term digital preservation if it commands adequate technical and organisational resources, operates according to its aims and policies and can demonstrate key measures of trustworthiness through transparency and supporting evidence. These latter features are vital: audit and certification behind closed doors is a club with a badge, not an open community with common practice.

Claims of trustworthiness of digital archives are easy to make but are difficult to justify or objectively prove. Over the past 12 years, digital repositories have focussed on an unstructured set of statements claiming OAIS conformance despite it being a reference model unsuited for compliance. For a decade, audit and certification have been treated as the prevailing methods for establishing their trustworthiness. The call for action in the 1996 report of the Task Force on Archiving of Digital Information (CPA/RLG 1996):

> *"A critical component of the digital archiving infrastructure is the existence of a sufficient number of trusted organizations capable of storing, migrating, and providing access to digital collections. […] A process for certification of digital archives is needed to create an overall climate of trust about the prospects of preserving digital information"*

was taken up by an international Digital Repository Certification Task Force, led by the Research Libraries Group (RLG) and U.S. National Archives and Records Administration (NARA) (Ambacher 2007). It developed a checklist for digital repositories that was published in 2007 as the *Trustworthy Repositories Audit and Certification* (TRAC) checklist (OCLC/RLG 2007).

A parallel initiative was started in 2004 by the German Network of Expertise in Long-term Storage of Digital Resources (nestor) that established a working group on the certification of trustworthy archives. Building on a draft version of the TRAC checklist, the nestor group focused on identifying features and values that are relevant for evaluating both existing and planned digital object repositories. The nestor criteria for auditing digital preservation repositories were published in 2006 (nestor 2006) and updated in 2008 (nestor 2008). On the conclusion of the nestor project, work on the trustworthiness criteria was transferred to the German national standards body and a new version of the criteria was published as a national standard DIN 31644:2012 *Information und Dokumentation – Kriterien für vertrauenswürdige digitale Langzeitarchive*.

These two texts formed a basis for an international working group to develop a new set of criteria on which full audit and certification of digital repositories could be based. This work resulted in 2012 with an ISO standard in support of the OAIS reference model: ISO 16363:2012 *Audit and certification of trustworthy digital repositories.* The same working group is working on an adjunct standard *Requirements for Bodies Providing Audit and Certification of Candidate Trustworthy Digital Repositories* (ISO/DIS 16919).[1] This standard will provide normative rules against which an organization providing audit and certification of digital repositories may be judged, and it describes the auditing process within the wider framework of the ISO 17021 standards for conformity assessment.

The checklists or metrics that TRAC, ISO 16363 (a major inheritor of the TRAC controls) and DIN 31644 provide as a basis for audits are presented as quality criteria that a trustworthy repository should meet. They provide digital repositories of all sizes with direction for demonstrating their adherence to quality and consistency, to respect for data integrity, and a commitment to the long-term preservation of and access to the information entrusted to their care. The metrics are mostly derived from practice and

[1] The DIS suffix denotes the current (March 2014) 'draft' status, but reflecting that it will become a standard.

reference the OAIS Reference Model (ISO 14721) and thus associate the concept of quality with the OAIS model's principles.

The criteria are divided into groups that reflect levels and types of activity involved in running a digital repository, for example (ISO 16363):

- Organizational infrastructure, that addresses issues such as governance and organizational structure, staffing, procedural accountability, the policy framework, financial sustainability, and contracts, licenses, and liabilities.
- Digital object management, that assesses the acquisition of content, creation of the Archival Information Package (AIP), preservation planning, the actual preservation of the AIPs, and the management of information (i.e., metadata) and access.
- Technical infrastructure and security risk management.

Two other initiatives have followed the self-assessment route and developed 'softer' methods for establishing and assessing quality of work in a digital repository. The *Digital Repository Audit Method Based on Risk Assessment* (DRAMBORA) (Hofman et al., 2007) presents a methodology that characterizes digital curation as a risk management activity in which the role of a digital curator is to rationalize the uncertainties and threats that inhibit efforts to maintain digital object authenticity and understandability, transforming them into manageable risks. The DRAMBORA on-line toolkit[2] facilitates repositories in developing their risk registers and publishing them as a form of transparency that engenders trust.

The *Data Seal of Approval* (DSA) method was initially proposed by the Data Archiving and Networked Services (DANS) in the Netherlands and includes 16 guidelines to help data archiving institutions to establish trustworthy digital repositories for research data. The DSA characterises the repository assessment as a two stage process in which a repository carries a self-assessment against the guidelines that is then peer-reviewed by a member of the international DSA assessment group. The reviewer recommends to the board whether the guidelines have been complied with and whether the DSA logo can be awarded to the data repository (Harmsen 2008, p. 1). The Data Seal of Approval does not include a site visit and relies on the availability of public documentation and the public nature of all self-assessment statements that result in a Seal being awarded as a means of ensuring trust in the process of peer-review.

Out of these five approaches to establishing the trustworthiness of a repository, a three-tier auditing and certification framework has emerged (European Framework 2010):

- Basic Certification should be granted to repositories that obtain DSA certification through a process of self-audit and the public release of a peer-reviewed statement from another organization which has previously received the DSA;
- Extended Certification is granted to Basic Certification repositories that also perform a structured, externally reviewed and publicly available self-audit based on ISO 16363 or DIN 31644; and
- Formal Certification is granted to repositories that in addition to Basic Certification obtain full external audit and certification based on ISO 16363 or equivalent DIN 31644.

Of these three levels, currently only DSA certification is operational and so far 24 organisations have received the Seal. Certification based on ISO 16363 can only commence once the associated standard ISO/DIS 16919 is completed and published.[3] The German nestor network has started a *nestor Seal for*

[2] http://www.repositoryaudit.eu/
[3] http://www.iso16363.org/preparing-for-an-audit/

Trustworthy Digital Archives scheme that is issued, for a fee, after successful extended certification.[4] The Center for Research Libraries (CRL) in the U.S. has been carrying out repository audits based on the TRAC checklist and has issued four certificates of a trusted digital repository based on this.[5]

Other international standards have been developed that discuss the design and operations of a digital repository. ISO/TR 17068:2012 *Information and documentation — Records management — Trusted third party repository for digital records* establishes trustworthiness criteria needed for reliable digital records management and specifies the requirements of a trusted third party repository (TTPR) services, system and management. The TTPR is thought of as maintaining digital records on behalf of the authoring agency and providing certification and notarization service for the records. The technical report describes TTPR services, system and management requirements; no TTPR conformance audit or certification is based on the ISO 17068.

ISO 14641-1:2012 Electronic archiving — Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation is originally based on a French national standard and describes the methods and techniques to be used for the implementation of an electronic information system for managing documents within an archive. Primarily it describes criteria for system design and specifications for operational processes that ensure legibility, integrity and traceability of the documents for the duration of their preservation. The standard describes a basic method for assessing third party service providers' compliance with the standard's requirements and lists elements of a typical service level agreement for service providers.

In addition to these standards and self-assessment methods designed specifically for organisations involved in digital preservation, digital repositories have found it advantageous to seek compliance with other standards that are widely accepted as proof of quality of work. For example, the quality management system series of standards (ISO 9000 family) that address quality assurance components and establish a system for continuous management of quality; the information security management system standards (ISO 27000 series) that seek to establish control over information assets; ISO 31000 series of standards on risk management; and ISO 30300 management system for records. All of these management system standards sets are highly relevant for any digital repository, but lack the explicit goal of establishing trustworthiness that has been sought after in the digital preservation community or fail to consider the long-term (preservation) aspects when discussing usability of digital assets.

The converse is also true of course—the close alignment to digital preservation needs of these standards would necessarily narrow their focus which in turn would de-value their more generic applicability. The final section of ISO 16363 may be more locally applicable to digital preservation needs but is unlikely to confer the same level of reputational increase as the ISO 27000 suite of standards if information security is a critical element of a repository's mission.

As standards emerge and gain adoption, best practices and agreed levels of compliance evidence are not immediately available. No matter the rigour or depth of a standard, it evolves in application and community guidance on meeting controls evolves alongside it. The standard itself is ideally in a state of continuous improvement as is the understanding of conformance to its controls through an audit process. In the curation community, whose stakeholders include the auditors, this emergence and adoption is in its early stages and will need to take account of existing quality standards in place.

[4] http://www.langzeitarchivierung.de/Subsites/nestor/EN/nestor-Siegel/siegel_node.html
[5] http://www.crl.edu/archiving-preservation/digital-archives/certification-and-assessment-digital-repositories

Establishing trustworthiness therefore is not (currently) a matter of just meeting the requirements of any single standard. Certain elements of trustworthiness for an organisation may be able to be demonstrated through a standard, but as two of the authors of this work have previously expressed it (Ruusalepp et al. 2012, p. 148):

> *"… as memory institutions preserve materials that other organizations have created, they also apply many standards that have been created by other communities. Digital preservation is an inclusive domain and as far as standards are concerned cannot (and should not) rely on its own standards alone. Learning to piece together the jigsaw puzzle of standards from different domains is a skill that every digital curation specialist needs to have, alongside the skill of discriminating between what is or is not locally appropriate."*

Furthermore, we believe that the application of standards is, more than notionally, related to the concept of quality.

2.2 Layers of trust in quality of digital curation

Trustworthiness as a concept has wide-reaching implications and is pertinent to relationships both internal and external to the repository. First of all, the management, staff, fund-makers and partners of a repository must all be satisfied that their efforts are capable of meeting formal mandates and expectations. Similarly, information creators, depositors and users are interested in obtaining similar assurances of the competencies of the organisations providing maintenance, preservation and dissemination services.

The original *Trusted Digital Repositories: Attributes and Responsibilities* (2002) report discussed trust-building on three levels:

1. How repositories earn the trust of their designated communities.
2. How repositories trust third-party providers.
3. How users trust the documents provided to them by a repository

The subsequent work on criteria of trustworthiness has in addition focused on the operational level of carrying out digital curation activities in a digital repository (cf. digital object management in ISO 16363 and DIN 31644). The stakeholders included in a typical trust network of a digital repository today can be grouped up to four types:

1. Data creators: for example, publisher, record-creating agency, donator, are typically interested in trusting the preservation and access services of the archive and ensuring the quality of their data;
2. Data users: for example readers, researchers, agencies, etc., are interested in trusting both the services and the data they get from the archive, and ensuring that both are of the highest quality;
3. Repository owners and/or funders: for example, government, shareholder, agency that the digital archive is part of, etc., are usually interested in trusting the services of the archive as a whole, and ensuring that its services and products are deemed of the sufficient quality;
4. Data rights owners: the subjects of a dataset held by data archives, an author of a book in digital libraries, citizens as co-creators of public records, are interested in trusting the organisation, the digital curation services, and ensuring that their data are being managed by processes which are of the highest standard.

Although the concept of services has not been elaborated in the context of trusted repositories, it is useful to view trustworthiness of digital curation as a layered concept that moves from macro level trust to micro level trust issues. Quality measures that inculcate trust may depend on the stakeholder, and indeed

may differ from stakeholder to stakeholder. For data users a trusted, usable, contextualised object is directly experienced and used; at the funder level the quality of individual outputs is harder to absorb and evidence of recognisable good practice in the development implementation and management of artefacts for processes and risks will have greater currency. Therefore, quality must exist at a variety of levels and must be evidenced and approved in different ways. Thus it can exist at a procedural pass/fail level or minimum standard reached, can be a machine actionable metric or could be a human actionable "this meets the expert consensus on quality" threshold (brings in skills and roles). It is only together that these various elements together confer a trust status.

The sections below identify three key areas for trust: the organisation, the business function, and lastly, the preserved material (data) itself.

2.2.1 Trusting the digital curation organisation

An organisation that takes on long-term responsibility for digital data is expected to demonstrate its sustainability and/or business continuity. Memory institutions often have their mandate embedded in legislation and have been in the preservation "business" for decades, sometimes centuries. Digital preservation institutions do not have a long track record yet—the oldest are not much more than half a century old—and often have to prove not only their competence but also their ability to maintain the preservation service. This extends to broader aspects than having technology solutions and includes broader organisational issues like legal legitimacy, adequacy of policies and availability of competence. In the business sector, enterprise risk management and business continuity / contingency planning methods are often used to meet the sustainability expectations of stakeholders. However, the standard methods for these—the ISO 31000 series of standards on risk management, and the ISO 22301 and ISO 22313 on business continuity management—do not cater specifically for preservation needs. The digital repository auditing methods do elaborate on the link between organisation and the preservation function and assess organisational viability from the perspectives of:

- Mandate or mission statement that reflects a commitment to the long-term preservation;
- Succession plan, contingency plans and/or escrow arrangements;
- Awareness of the legal and regulatory context that the repository operates in;
- Policies that reflect and support the mission to preserve;
- Clear identification of duties that need to be performed to carry out the mission and existence of staff with adequate skills and experience to fulfil these duties;
- An effective preservation policy;
- Commitment to transparency and accountability of decisions and actions supporting preservation;
- Financial sustainability of the organisation;
- Effective management of contractual obligations and outsourced services.

From the quality assurance perspective these questions help to determine how digital curation (business function or service) is embedded in the organisation as a whole is adequate and sustainable. A separate deliverable (D4.2) of the 4C project is exploring the models of sustainable digital curation within organisation.[6] There is a great diversity in how organisations curate their digital assets and combine the curation function with the rest of their business functions. No universally applicable metrics exist to assess the suitability of these business models and hence the auditing toolkits refer to the requirements derived from the external stakeholders (designated user groups) of the given repository. Furthermore these

[6] A draft version is available at: http://4cproject.eu/community-resources/outputs-and-deliverables/esrm-summary

concepts are not fully compatible with any 'distributed repository' scenario whereby multiple organisations operate consistently at the business level as a single organisation. Macro-level trust can here be seen as a process or interaction between client and service provider and is based on the expectations of the given client. While transparency has an enabling role in this interaction, since it can make 'trust' more public, it does not necessarily allow an organisation to convert 'trust' into a higher overall reputation, since reputation is based on multiple *interpretations* of trust.

2.2.2 Trusting the digital curation business function

Digital objects require management if they are to maintain their recurring value. Management of digital objects is at present done predominantly in digital repositories, mimicking the traditional approach of accumulating objects worthy of preservation into centralised collections managed by memory institutions. A number of process descriptions, models and diagrams have been proposed to support the integration of curation activities with wider repository processes, for example the Digital Library reference model developed by the DELOS and DL.org projects (DELOS 2007; DL.org 2011); the InterPARES project Chain of Preservation Model (InterPARES 2007); the UK Digital Curation Centre's Curation Lifecycle Model (DCC 2009); but the Open Archive Information System (OAIS) model (ISO 14721) that was originally published in 2001 retains its intended role as a common reference. The TRAC, ISO 16363 and to large extent DIN 31644 rely directly on OAIS definitions, concept and functions and the DSA was developed to present coverage of the functional entities and actors from OAIS within 16 guidelines. In the words of the TRAC checklist:

> *"TRAC's evaluative metrics should be used to judge the overall suitability of a repository as being trustworthy to provide a preservation environment that is consistent with the goals of the OAIS. Separately, individual metrics or measures from TRAC can be used to identify possible weaknesses or pending declines in repository functionality."*

The metrics in the audit checklists follow archival phase of the digital lifecycle covering the operations' level thoroughly. Effectively, the metrics are quality criteria for processes and operations of digital curation, as seen through the lens of the OAIS reference model, and should engender trust in repository's ability to successfully carry out digital curation.

Digital repository self-assessment methods (DRAMBORA, DSA) do not rely on a fixed model of repository operations and their criteria are designed to measure fitness for purpose of activities. The appropriate level of quality is determined by the repository itself taking into account its organisational context, types of preserved content, purpose and target audience of preservation.

The information security aspects and reliability of the technical infrastructure that support digital curation are also covered in depth in all audit checklists. Most metrics are overlapping with information security standards (e.g. ISO 27002) but vitally also include aspects of long-term preservation that do not feature in non-digital preservation standards.

Appropriate levels of quality at this level may be defined through organisational context at the macro level. The availability of quality of outputs at the micro level (see below) may imply quality and therefore trust at the mid-level but cannot guarantee it. Transparency of process, with common definitions, process descriptions and quality measures will support both effective audit outcomes and the transfer of good practice throughout the curation community.

2.2.3 Trusting the preserved data

Users must be able to trust digital objects provided by the digital repository. The repository's role is to ensure that significant properties of digital objects are maintained throughout cycles of active digital preservation that may change storage media, file format or other types of representation of the object. The TDR report (RLG/OCLC 2002) discussed questions like: How can a user be certain that the document received is the one requested? How can the document be verified to be the exact item deposited into the digital repository in the past?

A more recent focus of attention is the establishment of clearer data provenance to ensure that digital objects that have been combined, processed, transformed or migrated maintain their integrity. Provenance information includes but is not restricted to fixity checking. Provenance information is increasingly used as an indicator of data quality, not only in the maintenance of details of successive steps taken during curation but ideally maintaining details of methods, software and calibrations used. This is perceived as a difficult problem as it involves retention of detailed processes and values from the pre-repository phase of the lifecycle, but is particularly necessary for data with potentially a very long lifetime of usefulness, such as earth observation data; where complex processing has been carried out, when it might be necessary to distinguish different versions of software (Dallmeier-Tiessen et al. 2012, p. 69); or for the purposes of research integrity and reproducibility.

It is unlikely that a universal quality standard will emerge with exact criteria for assessing data quality from the user's point of view but those users are often those with the greatest direct contact with the data and the greatest facility for making cases by case data-level decisions about quality. By ensuring maintenance of adequate metadata about preservation actions applied by the digital repository will go a long way towards providing an audit trail of data provenance.

2.3 The quest for quality and trustworthiness—conclusions

Digital repositories can be large or small, handle a wide range of materials from cultural heritage, research, government, or business institutions; they have different organisational contexts and operating situations, technical architectures and institutional responsibilities. Defining a common 'yardstick' for measuring whether all the different digital repositories could be trusted by a wide array of different stakeholder groups is a challenge whose current proposed solution is to develop commonly-applicable quality criteria amenable to self-assessment and audit. The underlying concept of repository audit approaches is that a repository is trusted if it fulfils a minimal set of common criteria (as relevant as possible to all repositories) and can demonstrate its capacity to fulfil those specified functions.

The conferment of a recognition of success of digital repositories presupposes the availability of an objective benchmarking mechanism. The use of the OAIS model as a common reference provides a benchmark against which the audit methods may in turn be measured, or at least compared. Such a common reference and benchmarking is critical if audit outcomes are to be universally acknowledged. A key challenge for those developing repository audit tools has been to provide a sufficiently tangible structure for determining where conformity and success actually exist (McHugh et al. 2008). A consensus is gradually building around separating the quality criteria into layers of organisational viability, digital repository activities, technical infrastructure and data provenance. However, the same consensus is not emerging in terms of the transparency of the audit process itself.

The digital preservation community is not homogenous—memory institutions sit alongside research and government institutions, businesses, and service providers. Many of the standards that have been developed within this community deal with workflow control, but it is impossible to completely

homogenize preservation workflows across the whole community. The type of standards that the digital preservation community has agreed upon—what could be called voluntary compliance standards—are mainly suitable for improving work processes (in their broadest sense). However, the uniform use of voluntary standards is difficult to coerce. Conformity in all matters is not necessarily desirable, especially if the primary purpose of the activity of digital preservation is to ensure that the materials being preserved can be used at some defined point in the future for some particular purpose, and that the defined point in the future and the particular purpose will differ across organizations (Ruusalepp et al. 2012).

Maturity of digital curation as a domain in terms of standards development is an on-going process where auditing standards are applied and find their role within the activities of the community. The OAIS standard provided a common reference model (but not a full process or technical implementation standard) against which archives could benchmark their activities. Following this a range or trust-oriented evaluation standards are under development with peer-review and audit processes under deployment. As adoption increases and critical mass is reached the various stakeholders will evolve a position on how these standards fit into their practices.

These first generation audit and certification standards will themselves evolve, whether like ISO 16363 through a five year cycle, or faster for less formally developed approaches. Over time audit practices will determine the appropriate values to assign to the metrics in each standard and common approaches to developing compliant evidence will evolve. Such common approaches will by their very nature support the alignment of approaches to digital preservation practice that will in turn reduce the cost of certification.

These various trust standards exist within a wider framework of standards as outlined above. Over time papers, websites and other 'auditee' supporting materials will evolve to provide greater guidance on the application of trust metrics. This process will also identify community responses on how well the standards fit their needs, what level of certification is appropriate and how the trust standards compare to and interoperate with wider standards conferring quality assessments.

The maturity curve of applying standards in organisations starts from testing and benchmarking then moves through risk management towards quality management, eventually reaching an apogee in an organization capable of learning. Standardization in digital preservation is still at the beginning of this curve, focusing primarily on benchmarking the performance of curation tasks and beginning to look at risk management of preservation. An organization that is mature and able to adapt to changes is, however, looking more at efficiency of processes than controls over products (systems) and their interoperability. When moving from quality control to quality assurance to quality management, the management of people and skills becomes the biggest challenge, instead of technology and workflow. Reshaping an organization is more connected to its employees than the technologies it uses (Ruusalepp et al. 2012).

The same maturity curve seems also to be affecting the better understanding of the costs of these activities. Most organisations carrying out digital preservation welcomed the introduction of these methods of inculcating trust as a research activity rather than solely as a trust activity, hence the paucity of costs. Clearly, as digital curation becomes more mainstream, identifying costs for inculcating trust and improving quality will be more straight-forward, as they will be separated from standard organisational costs.

Finally, we should repeat ourselves: the formal checking of the quality of operations may enhance the reputation of a repository but trust *per se* should be engendered through measurable standardised controls. Reputation may seem to be synonymous with trust, but the relationship between them is vexed. Reputation may be enhanced by other factors, unrelated to quality—and often symbolic; trust can only be fully gained through evidence-based, independent audit activities.

3 Quality, Trust and Derived Benefits

Investment into quality assurance of a digital repository yields benefits not only to the digital curation service but also to the organisation as a whole (cf. D4.1). Applying quality management principles induce a strong customer focus, enhance the motivation and implication of senior management, support process approach and continual improvement (ISO, 2012). A by-product of introducing quality management and preparing for an assessment or audit is documentation that enables communication of intent, consistency of actions and which supports traceability. This documentation also provides enhanced business continuity, especially where staff-turnover reduces knowledge transfer.

Quality of service can be achieved or improved through application of best practice in activities and use of standard technologies. However, in order to make quality measurable it needs to be assessed against established set of criteria. The results of the assessment or audit process can then be communicated and verified through certification. Organisations seek certification for many reasons, as certification may:[7]

- be a contractual or regulatory requirement;
- be necessary to meet customer preferences;
- fall within the context of a risk management programme; and
- help motivate staff by setting a clear goal for the development of its management system.

In reality there are two main drivers for using digital repository audit methods; first, increased trustworthiness of the repository among its stakeholder groups and ultimately a higher reputation of the organisation; second, increased quality of processes being undertaken. The publication (transparency) of the audit results (i.e. assessment of quality) is also believed to lead to higher trust and reputation.

3.1 Trust-building through disclosure

The evaluation of repository's current practice against established (quality) criteria provides its users and stakeholders (cf. D4.1):

- higher confidence in reliability and authenticity of the digital objects that the organisation is providing to its clients (i.e. trust in data);
- higher confidence in services that the organisation is providing to its clients (i.e. trust in the digital curation service);
- higher confidence in the commitment of the organisation to seek continuous improvement of its work processes through application of quality procedures (i.e. trust in organisation).

The digital curation service is often not directed at external clients but is offering an internal service to the parent organisation. Quality of operation and service needs to be demonstrated to internal clients, too. Internal transparency of quality assessment ensures that management measures can be traced, effects of changes in economic scenarios can be evaluated, and documentation of quality can be shared with operators, funders, management and employees.

Attaining trust status is not a one-time accomplishment; to retain trustworthy status, a repository will need to undertake a *regular* cycle of audit (CCSDS 2009). Each audit can only measure a snapshot of the current state of quality; continuity of practice is assessed based on any policy framework enforced in the repository.

[7] http://www.iso.org/iso/home/standards/certification.htm

In the course of an audit some hard evidence (facts, observation, direct experience) will be collected which —on the societal level—is commonly accepted as the main source of trust. Nevertheless, it is unlikely that an audit here and today will remove all doubts about repository's ability to deliver a service in the future. The type of trust repositories are expected to demonstrate is 'dispositional trust'. It is the trustor's belief that it will have a certain goal B in the future and, whenever it will have such a goal and certain conditions obtain, the trustee will perform A and thereby will ensure B. This generalised expectancy—dispositional trust—is operational when a decision to trust or not to trust is made in the absence of direct evidence as to whether another is or is not trustworthy (Rotter 1967, p. 651). In the context of digital repositories we are almost invariably talking about the dispositional type of trust—when we consign our material to a repository we trust the repository to carry out active digital preservation actions on our deposited content in the future. Hence, our trust expectation is directed towards the future activities of the repository, and we have very little (and sometimes no) evidence at hand that these activities will result with a successful outcome. The digital preservation community has not yet developed a practice for collecting evidence base for successful and unsuccessful digital preservation actions. The repository audit is, therefore, by default left with observing the current behaviour and studying documentary evidence on repository activities, and making only predictions on the future reliability of the repository services based on policies. Reliance primarily on dispositional trust introduces uncertainty and risks into the audit outcomes, making also the certification of repositories questionable and, indeed, risky. The nature of auditing as a generic verification method that does not cater well for deciding on adequacy of future activities, services or states of affairs places high requirements on efficient and effective set of policies in the repository in order to demonstrate the ability to maintain the level of quality that an audit has verified.

A number of trust models have been developed for automated environments where decision-making to trust is based on quantified measures (see Salo, Karjaluoto 2007; Debenham, Sierra 2008; Li, Ping 2009; Shekarpour, Katebi 2010). These models include a 'protocol' that is used to communicate the information components that enable a decision to be reached whether to trust or not a service. With the ISO/DIS 16919 still in development, the digital repository audits have, as yet, no fixed agreement over the protocol that should provide the stakeholder communities with confidence for trust decisions. Each audit tool has its own mechanisms for reporting on the audit findings and the amount of evidence presented in the reports.[8] There are risks associated with repository audits, which may also have a relationship with the level of transparency required in the process:

- **over-confidence:** clients will put more trust in a repository than it deserves, or have not considered all the risks involved or are willing to take more risks. The result of this can be that the repository turns out to be unreliable or incompetent, or the client does not have sufficient control over (poor) service the repository is providing, or a service contract is signed that does not cover all likely eventualities or includes misunderstandings;
- **over-diffidence:** insufficient confidence in repository. The result of this can be that the client will miss a good service—a long time can be spent on searching for additional evidence or proof; client is trying to instil too many controls over quality of service which cost extra time and money; client prescribes too much to the repository without relying on its competence to do its core business.

Independent certification mechanisms are designed to assist in overcoming these types of risks and to provide uniformity to disclosing information on audit results.

[8] The ISO 1636 example audit report template was published as Annex B of the APARSEN project deliverable D33.1B *Report on Peer Review of Digital Repositories* (APARSEN 2012)

In this context full transparency is interesting. There is an illusion that full transparency always leads to greater trustworthiness. Transparency may cause both over-confidence and over-diffidence depending on whether the level of understanding that the trustor has over the processes which the repository is supposed to be carrying out. One repository manager noted that their funder said they trusted them more because they published their policies on the web. The funder had no ability to discern whether or not those policies were being appropriately implemented!

3.2 Benefits from seeking certification

Certification is the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements.[9] Certification is a mechanism through which organisations can obtain a qualification that their products, operations and services comply with a standard. Having audited and certified quality management systems can provide competitive advantage in the market and contribute towards increased reputation of the organisation.

As noted above (section 2.1) across the five referenced methods for demonstrating trustworthiness of digital repositories there are two different approaches to audit: verified self-assessment and formal audits. These approaches were positioned into three hierarchical levels in a memorandum of understanding signed in 2010 between the groups working on audit methods.[10] The "Basic certification" under the Data Seal of Approval represents a verified (peer-reviewed) self-assessment whose statement is made public once the Seal is granted. All subsequent levels of certification 'within the framework' imply the continued presence of a public DSA assessment though there are no barriers to adoption of the other methods independent of the Framework and therefore independent of the DSA. The "Extended certification" represents a verified (plausibility-checked), publically available self-assessment and "Formal certification" stands for an audit by external experts undertaking a standard-compliant audit process. Extended and formal certification are extensions of the Basic certification and both can be issued on the basis of DIN 31644 or ISO 16363. The German network of competence in digital preservation *nestor* has instituted a *nestor Seal for Trustworthy Digital Archives* that is issued after successful extended certification (nestor 2013). In the U.S. CRL has been issuing TDR certificates on the basis of TRAC audits. ISO 16363 is awaiting approval of the associated audit standard (ISO/DIS 16919) before offering certification services.

The choice of certification process and choice of approach to audit are important, because it is possible to undertake a self-assessment against ISO 16363 but not be formally audited (see section 2.1), and thus gain much of the benefit from undertaking the self-assessment but none of the formal benefits of being certificated against a standard. Similarly, an organisation may elect not to be formally audited against a standard owing to the actual cost of employing formal auditors. (The CLOCKSS archive's formal audit, without associated consultancy or staff time, cost c.$45,000 in 2013; the UK Data Archive's six-monthly surveillance audit for ISO 27001 cost around £2,500 a time, again without internal effort.)

The various certification types also engender different levels of transparency. If there are parts of documentation in the organisation or in the audit reports that are not suitable for the general public (e.g., business secrets, security-related information), these can still be requested and made available to a specified group or body (e.g., certification agency) (Dobratz et al. 2010, p. 49). The DIN 31644 and ISO 16363 standards are protected by copyright which produces a barrier to transparency. An organisation

[9] http://www.iso.org/iso/home/standards/certification.htm
[10] http://www.trusteddigitalrepository.eu/Site/Memorandum%20of%20Understanding.html

wishing to publish the results of their audit processes would be obliged to remove any controls/metrics reproduced from the standard.[11]

The risk assessment using the DRAMBORA method will provide repositories with:[12]

- A documented self-awareness of their fundamental objectives, and of associated activities and assets. By defining their operational contexts, organisations are well positioned to determine their own assessment parameters as well as verify that their resources are optimally invested and positioned to ensure success.
- A documented understanding of the risks they face expressed in terms of their likelihood and potential impact. Mapped to organisational aspirations and efforts this will facilitate subsequent organisational development and resource allocation, and offer a quantifiable insight into the contemporary severity of risks faced.
- Definition of their chosen means for risk management, determining the appropriate strategies for avoidance, treatment, transfer and tolerance, as well as the mechanics of their implementation. This process, which should be repeated on a regular basis, will provide opportunities to establish and achieve quantifiable targets, facilitating the on-going development of every aspect of organisational activity.
- DRAMBORA is a worthwhile precursor to external audit, accreditation, and certification when these services become broadly available.

The self-assessment using DSA provides positive results for several repository stakeholders:[13]

- Gives data producers the assurance that their data and associated materials will be stored in a reliable manner and can be reused.
- Provides funding bodies with the confidence that data will remain available for reuse and their investments will not be lost.
- Enables data consumers to assess repositories where data are held.
- Supports data repositories in the efficient archiving and distribution of data.
- Supports comparison through public statements engendering trust in the process and sharing current practice.

The benefits arising from formal certification have summarised for repository managers as:[14]

- something to show to funders and users;
- advice of where improvements are needed as some of these recommendations may be a revelation to the repository managers, others may be well understood and be helpful to those managers to make the case for additional resources or changed priorities to their funders.

[11] Interestingly, the *Audit and Certification of Trustworthy Digital Repositories. Recommendation for Space Data System Practices* (CCSDS 2011) is freely available on-line without a copyright statement, and is identical to the published standard. It would be hard for ISO to prove mis-use of copyright.
[12] http://www.dcc.ac.uk/node/9589
[13] http://datasealofapproval.org/en/information/about/
[14] http://www.iso16363.org/benefits/

The stakeholders who fund repositories or deposit their content for preservation to repositories should benefit from:

- re-assurance where it is warranted—and warnings where trust is not warranted, gives some comfort that someone besides the repository managers can tell them that the repository has (or has not) been doing a good job;
- this goes beyond simply how well the bits will be preserved, instead the reassurance is that the digitally encoded information will be usable into the future;
- rather than a simple yes or no, the audit identifies areas which need improvement.

The currently work-in-progress draft ISO/DIS 16919 *Requirements for Bodies Providing Audit and Certification of Candidate Trustworthy Digital Repositories* provides normative rules against which an organisation providing audit and certification of digital repositories may be judged, and it describes the auditing process. Once formally approved and published by the ISO as a standard, the formal certification of trusted digital repositories can commence and new benefits will emerge on the digital curation market.

3.3 Stakeholder reports

In 2008 nestor network conducted a series of interviews in Germany to ascertain the level of usage of quality-related standards in digital preservation organisations. The study concluded that (Dobratz et al. 2010):

> *"Public institutions didn't recognise an advantage for themselves, their services, and customers in being certified for ISO 9000 (2000) or even as trustworthy digital archive. The portability of quality management standards to the procedures and services in public administration is considered as virtually impossible. Often the enormous complexity of standards is seen as the main barrier to complete compliance. Instead, standards are (mis-)used as guidelines and their principles applied to selected workflows and processes: documentation, transparency and quality control of ingested objects. […] Most institutions have already thought about quality management, discussed the applicability of standards and elements derived from those standards, and follow their own interpretation of quality control and management. The study reflected a strong demand for deeper and broader information on standards as well as support and training during the introduction of standards."*

The absence of guidance on applying quality standards to digital curation led some institutions to try a multitude of quality criteria. For example CINES (Centre Informatique National de l'Enseignement Supérieur) has over the years applied four of the assessment methods described above, plus a French national standard on specification of a digital archive that has since become ISO 14641-1 (Bechard, Massol 2012). The incentive for such an extensive investment into quality assurance came partly from the legal mandate of the digital curation service that set long-term requirements, and partly from in-house levels of quality applied to performance and risk management. The benefits of these assessments for the organisation were continuing funding ("the final objective was the realistic evaluation of the services provided to the communities"), new business opportunities (services for new types of content and new client groups) and a strong position for participating in the discussion of repository auditing and certification internationally.

The certification of repositories based on the TRAC checklist was borne out of a practical need; when library budgets shrank leaving less money for acquiring and preserving paper publications, the need to rely on digital publications grew and with it the need to trust CRL partner organisations to maintain the availability of these publications over the long term.

> *"In today's economic climate libraries must realize the greatest possible return on their investment in electronic scholarly resources and digital preservation services, and need to move aggressively to reduce the costs of redundant print holdings. Certification augments CRL's strategic archiving of print and supports the responsible transition by CRL libraries to electronic-only formats where appropriate."*[15]

The TRAC-certified repositories have reported benefits on the level of gaining competitive advantage and attracting new customers:

> *"This is a crucial milestone for Portico, and one we hope will provide libraries and publishers with even greater confidence in our ability to serve your preservation needs over the longterm"*[16]

> *"OCUL hopes its example is a source of encouragement for others considering long-term digital preservation endeavors."*[17]

The audit process and preparation for certification itself had positive impact on the organisations:

> *"[The audit] confirmed that the majority of our practices conform to the Trustworthy Repositories Audit and Certification Checklist (TRAC) and other metrics developed by CRL through its analyses of digital repositories. It also identified for us several areas for continued improvement as well as ways in which we can enhance the service for CRL member libraries as well as others."*[18]

> *"Chronopolis see [TRAC certificate] as a important validation for the work we have been doing and a valuable guide for our future work."*[19]

But this impact was also visible for organisations in other areas, through the identification of inefficient processes, the development of more focussed and interconnecting policy frameworks, and even in one case a significant alteration in the planned changes to the overall business model of the organisation.

Audit reports that lead to TRAC certificates are publically available[20] and several repositories have also published their self-assessments.[21]

At present 24 organisations have obtained the Data Seal of Approval[22] and a further 10 are being peer-reviewed.

[15] http://www.crl.edu/archiving-preservation/digital-archives/certification-and-assessment-digital-repositories
[16] http://www.portico.org/digital-preservation/news-events/news/general-news/portico-certified-as-trustworthy-digital-repository-by-the-center-for-research-libraries
[17] http://www.ocul.on.ca/node/1637
[18] http://www.portico.org/digital-preservation/news-events/news/general-news/portico-certified-as-trustworthy-digital-repository-by-the-center-for-research-libraries
[19] http://chronopolis.sdsc.edu/trac/index.html
[20] http://www.crl.edu/archiving-preservation/digital-archives/certification-and-assessment-digital-repositories
[21] http://www.portico.org/digital-preservation/wp-content/uploads/2009/10/CRL-Audit-Portico.FINAL_.pdf; http://www.hathitrust.org/trac; http://chronopolis.sdsc.edu/trac/chronopolis_TRAC_self_audit.pdf; https://spotdocs.scholarsportal.info/display/OAIS/Document+Checklist
[22] http://datasealofapproval.org/en/assessment/

The benefits of obtaining a DSA status have been described by some of the DSA-repositories as:

> *"Emphasis on raising awareness and transparency is great, interaction with peer reviewer is meaningful and the Seal carries meaning that is easily recognized" (ICPSR)*[23]
>
> *"Put simply, we wanted to reflect on our own performance and we also wanted to be able to demonstrate to our peers and user base that we were a trustworthy repository for their data.*
>
> *Internal Review—undertaking the work toward the DSA enables us to reflect on the way we work and review our policies and procedures. In such a fast changing sector it is always beneficial to take time to consider whether we continue to meet the standards as they develop.*
>
> *Establishing bona fides—having the DSA will enhance our reputation both within our designated subject based community (archaeology) and within the wider world of digital preservation. The DSA will be a useful benchmark for comparison with other archives.*
>
> *Enhancing the trust of our users—digital archives, by their nature, do not benefit from having a long track record of sustainability unlike their counterparts in the world of traditional paper archives who have built up trust with both users and depositor, sometimes over several centuries. The DSA enables us to demonstrate to both the users of our archive and depositors to our archive that we are working to a set of standards and have been judged to have met those standards.*
>
> *Building a community—gaining the DSA embeds us within a community of archives working to higher standards and potentially allows us to benefit from closer ties and relationships with them. It opens up possibilities of working with others to enhance our policies and procedures." (ADS)*[24]

Since formal certification based on the ISO 16363 standard is pending on the completion and publication of the ISO/DIS 16919 standard, the participant comments are available only from pilot audits using ISO 16363. Six pilot audits with ISO 16363 were conducted as part of the APARSEN project in 2011, three of them in Europe, and the results are summarised in the project deliverable D33.1B (APARSEN 2012). The German National Library piloted the DIN 31644 standard and their evaluation of the audit process is described in the same deliverable. The APARSEN report will not be repeated here (please refer to Chapters 5 and 6 in the APARSEN D33.1B *Report on Peer Review of Digital Repositories*). The European repositories that participated in the pilot audits (UKDA, DANS, CINES) all reported benefits for their management of digital curation both on organisational and work processes level. The three US repositories were not APARSEN partners but indicated they sought some form of accreditation for a variety of reasons including the desire to demonstrate to management and reviewers that they were willing to undertake external, independent, international (ISO) evaluations in order to reach the highest standards in digital preservation.

The 4C project conducted interviews with stakeholders and collected written testimonials from organisations that have undergone a trusted digital repository audits (see the questionnaire in Annex 1:) to gauge further details on incentives and benefits of seeking certification based on standards. Some responses are listed below:

[23] http://www.datasealofapproval.org/media/filer_public/2013/09/20/5_icpsr_dsa_conference_florence_2012-mary_vardigan.ppt
[24] http://www.dcc.ac.uk/resources/case-studies/ads-dsa

"Our motivation for engaging in audits and seeking external assessment:

- *Systematic review of status quo*
- *Have our processes and documentation reviewed, scrutinized, and ideally approved by external professionals*
- *Determination of strengths and gaps*
- *Transparency towards the preservation community*

After the pilot audits and receiving the DSA we saw as additional benefits:

- *Assessment exercise and policy follow up raised the profile of long term preservation within the organisation (higher management)*
- *DSA as a solid basis for assessment against DIN 31644*
- *Renewal of DSA will hopefully document progress made" (DNB)*

The UK Data Archive found similar benefits to the DNB, and additionally felt that the DSA had the potential to provide a greater level of trust and interoperability across the group of 13 CESSDA Service Providers. DSA provided a framework of commonality that could be used beneficially by both mature and less mature organisations.

Through discussions with stakeholders we have learned of other quality-related standards that digital repositories have applied and the benefits they have reaped from doing so:

"By applying the ISO 27001 information security standard to the entire organisation's IT infrastructure and undergoing a formal audit process, a digital archive was qualified to bid for hosting a national service." (a data archive)

"Applying the national information security standard and getting a certificate to prove this have become a pre-condition for receiving additional funding for IT systems' development." (a national archive)

"Quality assurance increases the chances of re-using the data." (a data archive)

"It's a simple matter of publishers trusting us not to misuse or be susceptible to a malicious attack that results in misuse of the in-copyright digital publications they have deposited with us. This trust starts from the level of IT and information security that we have to prove to publishers in the first place. Having an information security audit certificate is a must for us." (a national library)

"Ongoing self-assessment to TRAC has reduced the risk caused by staff churn, and improved internal staff communication." (a data archive)

"Since 2007 it has been mandatory for all government agencies to comply with the national information security standard that will be replaced with the ISO 27001 in the near future." (a national archives)

"Information security standards include a number of requirements, which require considerable financial resources and a lot of human resources. But overall they seem rather reasonable without being too rigid—after all we are not building space rockets or running a bank." (a university library)

"Self-assessment to TRAC is uncovering inefficiencies in service provision which are not directly addressed by the standard." (a data archive)

Clearly repository managers have an understanding of the benefits of some form of assessment and audit and certification. Many of these are not related directly to trust, but to the identification of both better quality practices and more efficient practices. However, very few of the organisations we have spoken with have identified significant cost savings as a consequence of these activities, only *additional* costs. Some see these additional costs as being beneficial to the overall practice of digital curation, others believe that it gives them a competitive advantage, yet others believe its essential investment in maintaining a leadership role.

3.4 Benefits from quality and trust—conclusions

A decade ago the ERPANET project discussed the incentives for auditing digital repositories and predicted that there will be clear need for them in the near future (ERPANET 2004):

> *"So what is the value of audit for digital preservation? The longstanding experience of traditional memory organisations, combined with their responsibility has given them a veil of sanctity with respect to trust, therefore audit has been rarely used. So what, if anything, has changed? Besides the fact that digital resources are much more vulnerable than traditional paper based documents, it may be that the new digital order has made people and organisations insecure about their use of technologies, whether their methods and procedures are sufficient and effective, and whether both of them can guarantee the authenticity and longevity of the digital objects they are responsible for."*

Today we see the concept of auditing becoming part of the mainstream dialogue in digital repositories and the potential motivations for undertaking audits are diverse. Most organisations undertaking audits will make a business case for undertaking the audit on a combination of these:

- to improve the work processes;
- to meet a contractual obligation;
- to provide a publicly understandable statement of quality and reliability.

4 Cost of quality

4.1 Introduction

The digital preservation cost models do not explicitly include costs for activities solely related to trustworthiness or quality. The 4C project gap analysis of digital curation cost models (D3.1 *Evaluation of Cost Models and Needs & Gaps Analysis*) identified the lack of the cost models' capability for expressing the quality of digital curation activities and services as a "prominent gap" and suggested that the adoption of audit and certification practices might help bridge this gap.

The only known cost model which includes an implicit understanding of costs relating for trust is the *Cost Model for Digital Archiving* (CMDA)[25] which makes certain assumptions about the organisation under observation having "the philosophy of a trusted digital repository (TDR) compliant with the 16 guidelines listed in the Data Seal of Approval (DSA)" (Palaiologk et al. 2012, p. 212).

In two recent reports the APARSEN project presented a benchmarking exercise of digital preservation cost models against the ISO 16363 standard (APARSEN 2013a and 2013b). This was done by mapping the activity breakdown of the models to the activities framed by the standard, namely the activities within the three main sections "Organisational Infrastructure", "Digital Object Management" and "Infrastructure and Security Risk Management", as well as the sections' sub levels. The report concludes that relating the costs to benefits on quality of operations is still an undefined area that requires further research (APARSEN 2013b, p. 34):

> *"A cost model describes only the relationship of activities to costs, and does not cover all aspects of the full business case, such as scope, constraints, assumptions, benefits and measures of success, quality management, options appraisal, value for money and risks. During the development of cost models it is presumed that the preservation rationale and benefits will have been separately developed, and will be implicit in the activities of the cost model."*

Improving the quality of work and services is often associated with higher cost or at least significant start-up investment. In the digital repository context such investments are weighted against potential benefits arising from, for example higher trust from stakeholders and other indirect or diffuse results that often presume long-term investment. Hence, putting a price tag or a ROI (return on investment) ratio on applying a standards-based quality measure is near to impossible, as it will vary from one organisation and its business case to another. The 4C project is, nevertheless, making a start on clarifying the economics of the first stage of the longer process of quality assurance—the audit and certification costs.

4.2 Data collection

A short questionnaire was designed for repositories to capture information on the costs of audit and certification. The questionnaire was constructed in such a way as to be as generic (i.e., non-'standard' specific) as possible and as granular (i.e., associating costs with 'low' levels of activity) as possible. The questionnaire was also designed from an objective point of view, which is that it was not created from an examination of known or existing evidence but from an examination of the key activities that would most likely provide an input into a cost model. The full questionnaire is reproduced in Annex 1:.

[25] http://www.dans.knaw.nl/en/content/categorieen/projecten/costs-digital-archiving-vol-2

The first section of the questionnaire was designed to document the organisational context of the audit and to understand some key factors that may affect the costs of the exercise. The second part of the questionnaire attempted to gather information on both the time used to carry out and implement an audit process and the direct cost of those activities. The questionnaire ended with questions about the post-audit process and costs related to maintaining the received certificate.

During the testing of the questionnaire with the 4C project partner organisations it became apparent that collecting all the evidence on audit costs for the survey is time-consuming and involves several experts within the organisation. Nevertheless it was decided to contact approximately 40 organisations that had been shortlisted by the 4C task members as having undergone an audit and ask them to participate in the survey. All of the organisations that responded (only 7) felt that the form of questioning was correct and that it attempted to elicit the right information, but timeframes were limited and none was able to provide the granular detail that we felt was necessary to make constructive comparisons between organisations. Most of the respondents estimated that it would take two to three months to gather all the required data. This period extended beyond the delivery deadline of this report and would have left us without empirical basis for our analysis.

As soon as these issues became fully apparent which was, unfortunately, rather late in the process, we reconsidered our methodology and focussed on carrying out a more qualitative approach. We carried out interviews with a series of senior digital repository managers, who were known to have carried out some form of audit and certification process and specialists within the digital curation domain. The questionnaire (see Annex 1:) was used as a template for interviews. We also set up a focus group to discuss our preliminary findings in depth with our advisory board members representing funding organisations (with responsibility for data archives) and this discussion is summarised in the next section. The qualitative data have informed our audit cost study and have been used to inform and confirm some of our conclusions.

4.3 Audit and certification cost variables

The questionnaire for collecting audit cost data reflects the main cost elements involved in carrying out an audit and being awarded a certificate. On the basis of this structure, the main areas are discussed below in sequence from the point of view of how they affect the economics of being audited.

4.3.1 Organisation Type and Scope

The type of organisation, whether national archive, national library, multi-discipline repository, subject based repository, institutional repository, commercial service provider, will affect the costs of audit and certification in many ways. Organisation type may be a key driver in the motivation to undertake audit and certification activities. The legal or regulatory framework or mandate of the organisation may necessitate the audits and at fixed intervals. The boundaries of the digital repository within a wider organisation can also determine the costs of an audit.

Audit and certification activities are more likely to be applied within smaller organisations where the barrier to innovation is lower; or in organisations which have some form of contractual mandate to carry out certification processes. For example, organisations that have some form of security mandate are required by data producers and sometimes the law to undertake some form of (information or IT) security certification. Conversely, organisations that have a legal mandate to preserve records are not usually required to undertake any form of trust certification.

A number of the organisations who we discussed these issues with also confirmed that the undertaking of multiple self-assessment / audit processes had a significant impact on the costs of any subsequent activity. Therefore ICPSR which carried out a self-assessment against the TRAC checklist in 2005-6, found that its costs for self-assessing against DSA in 2009 was a lot less than it would have been if the earlier self-assessment had taken place. Not only were the overall costs less, the ratio between preparation of evidence and the follow-up activities was entirely reversed.

4.3.2 Audit / Certificate Type

The three levels of audit and certification described above (see sections 2.1 and 3.2)—self assessment as basic certification, verified or peer-reviewed self-assessment as extended certification, and formal certification based on audit by external experts—also have different levels of associated costs.

Self-assessment is usually undertaken as an internal exercise although it may involve external experts as facilitators of discussion. The results of self-assessment can often be documented and acted upon using traditional internal means and decision-making mechanisms. Once external verification of self-assessment results is sought, more effort will go into documenting the assessment and preparing documents regulating the repository work within the organisation. Costs on ensuring transparency of policies and activities will go up together with the level of certification.

Formal audit will involve the cost of contracting external auditors to carry out the evaluation and in some cases the price of the certificate issued. In some cases consultants with audit experience are also hired to help prepare for the audit process, which may have a significant impact on costs. (Consultants may cost more per day than internal staff but are generally more efficient because of their experience. However, internal staff are generally a fixed organisational cost, whereas consultants are more likely to be an additional cost.)

The effort required for a repeated audit or renewing certification is usually considerably lower than the first assessment. In other words, preparedness of the organisation and previous assessments and/or certifications undergone can significantly lower the costs.

4.3.3 Scope of Audit

The audits to establish quality management system or trustworthiness of a digital repository cover the entire organisation. DIN 31644 explicitly states that “assessment covers both organisational and technical aspects; it is not possible to assess merely one part of a digital archive (e.g. only the archive storage)” (nestor 2013, p. 3). For self-assessment, risk assessment or security audits it is possible to determine a narrower scope, for example, a single repository function (e.g. ingest), a component system (e.g. storage and back-up solution), or a particular service (e.g. e-journals access service). Understandably, a narrower scope offers savings in terms of staff time involved in the assessment and preparation of documentation, but may fail unveiling issues in the bigger picture or a whole workflow.

4.3.4 Temporal and Monetary costs

According to the APARSEN project effort expended in TDR assessment activities can be broken down into the following major areas (APARSEN 2012, pp. 22-23):

- preparation of evidence
- assessing level of conformance to the standard
- creation of new evidence if it does not already exist;
- changing policy/procedures if the procedures do not meet the standard (pre-audit)
- implementing policy/procedures

A finer-grain taxonomy of audit costs was used in the questionnaire for this task that distinguished (cf. Annex 1:):

- Resources:
    - Internal staff
    - External staff (consultants)
    - Equipment
    - Hardware
    - Software
- Activities requiring staff time when preparing for audit:
    - Preparation of evidence/documentation
    - Creation of an asset inventory
    - Interviews with staff
    - Assessing level of conformance to the standard
    - Creation of new evidence if it did not already exist
    - Risk assessment
    - Changing policy/procedures if the procedures do not meet the standard
    - Implementing policy/procedures
- Activities requiring staff time during the actual audit/certification process
    - Analysis of evidence and producing the evidence
    - Interviews and discussions
    - On-site audit/certification support
    - Follow-up activities after the on-site visit
- Post-audit/certification activities
    - Adjusting policies and practices, including the maintenance of the quality management system established for audit
    - Maintaining and updating the evidence base and documentation to support follow-up audits
    - Any additional costs

These cost categories are agnostic of the type of audit or standard applied. Combined with the type and scope of the audit exercise they should provide an adequate tool for planning and budgeting the audit. The organisational context—total number of staff, the legal requirements, the designated user community also affect the level and spread of audit costs and the ability to produce activity based costs. The level of support that audit can receive from records management and other support-activities or infrastructure services of the organisation can also significantly vary the cost of the audit.

4.4 Audit and certification cost estimates

The analysis of available audit and certification cost data remains a work in progress because the authors were unable to meet their own exacting levels of analysis for three main reasons. The first is the paucity of publically available cost information; the second is the lack of comparability of the cost information available. Owing mainly to the sensitivity of some of the information that has been received, it has proven impossible to present cost information at the level of granularity at which we had originally expected. The third reason is that ISO 16363 not reached the level of implementation maturity that we expected it would have by the time this report was being written. Therefore, our evidence for the costs and benefits of the implementation of this standard is based solely on the test audits undertaken as part of the FP7 APARSEN project, which was focussed on test deployment of processes from the auditor rather than the auditee perspective, and where the capturing of costs of activities was not the primary focus of the test.

Our questionnaire attempted to gather information on both the time used to carry out and implement an audit process and the direct cost of those activities.

4.4.1 Costs associated with resources

The first cost has been the procurement of standards that the organisation will be audited against. In some cases (for example, ISO 27000, ISO 9000) toolkits are available, for a fee, to guide and support the preparation for an audit and self-assessment. Hiring external experts and consultants has usually come at a higher fee than the user and guidance manuals although can provide advice tailored specifically for the organisation. On-line toolkits that facilitate self-assessment also exist for DRAMBORA,[26] DSA[27] and TRAC.[28]

Investment into new equipment has not been significant in the interviewed repositories (with one exception). In the case of information security audits some additional security-related software or installation for physical security had to be purchased. One repository reported the need to develop their repository management software at a significant cost in order to comply with the OAIS reference model requirements. However, the developed functionalities were already in the product development roadmap and their realisation had to be simply expedited which also brought the associated development cost forward in time. Platforms and tools for document co-creation and sharing (e.g. wikis) are available for free, but may have a staff development cost.

None of the interviewed organisation hired new staff to support the audit process directly, but a dedicated member of staff can spend a significant proportion of their working hours (50%-100%) on leading the audit project. Such displacement of existing staff from normal duties further complicates the calculation of overall cost. One organisation did hire a Digital Preservation Officer after their self-assessment against TRAC.

4.4.2 Staff costs

Staff costs are the predominant expense related to audit and therein relies also the difficulty in making the collected data comparable. The costs of staff vary considerably across countries, and the roles of staff required may range from senior management to administrative staff it is hard to get a clear picture. Two staff in the same organisation, doing identical activities may have salaries more than 10% apart owing to length of time employed.

[26] http://www.repositoryaudit.eu/register/
[27] http://assessment.datasealofapproval.org/accounts/login/
[28] https://www.archivematica.org/wiki/Internal_audit_tool

The length of the audit period, including the preparation, can be quite long. Staff engagement will vary throughout this period totalling on average 2-3 months FTE. Some examples from completed trusted digital repository self-assessments and audits are shown below. These are highly impressionistic figures which do not take into account any earlier self-assessments or audits, and from interviews it is clear that precision is impossible. The margin of error elicited in the questioning of one repository manager when asked twice over an two hour long interview was around 100% for an activity, thus *"about three weeks"* became *"three months of my time, and about half that of three others."*

Organisation	Type of audit	Duration of the process	Total staff effort
Portico	TRAC certificate	10 months	
HathiTrust	TRAC certificate	14 months	
Chronopolis	TRAC certificate	14 months	
Scholars Portal	TRAC certificate	6 months	
DANS	ISO 16363 pilot audit		3 PM
CINES	ISO 16363 pilot audit		3 PM
UKDA	ISO 16363 pilot audit		2 PM
DNB	DIN 31644 pilot audit		1.5 PM

Table 1—Audit effort and duration

The UKDA's originally submitted report for the ISO 16363 pilot (or test) audit stated:

> *"Two key staff members were responsible for the process with a review of the standard by staff responsible for key relevant areas. We would estimate that sixty person days of effort were expended on the process leading up to the arrival of the external audit team with ten person days of effort thereafter. The preparation took place in the context of the Archive's on-going periodic review and update of controlled documents and the revision of materials required for our forthcoming surveillance audit against ISO 27001, and may thus be a high estimate. However, we would expect that this process would have been considerably more time-consuming without previous certification against ISO 27001 or some other audited process which included a detailed risk assessment of the Archive."*

Furthermore, the UKDA had already undertaken a self-assessment against the DSA.

The National Library of Germany summed up its staff costs related to the pilot DIN 31644 audit as:

> *"Several staff members of the DNB were involved with varying intensity in the test audit. The DNB does not have a dedicated Digital Preservation unit, but staff that has to do with digital preservation is distributed over several units in the IT department. Preparations for the Certification Process were co-ordinated and mostly executed by one unit. Staff from the other units participated in a meeting to review and discuss the information to be submitted for the External Audit (plus some time for preparation and rework) and in the Formal Audit (plus some time for preparation). The Head of the Department supervised the process. In total 212.5 hours were spent working on preparing and conducting the audit. This corresponds to 1.51 person months."*

4.4.3 Certification costs

Many certificates incur a fee that can include only the administrative cost of issuing the certificate or also be inclusive of the site visit by external auditors for a fixed period of time.

The trusted digital repository self-assessments (DSA, DRAMBORA) have no fees associated with them. The nestor Seal for Trustworthy Digital Archives currently costs 500 Euros.[29] This includes the review of the self-assessment results and the right to publicise this by using the nestor Seal (e.g. on organisation's website).

TRAC certificates are issued for a fee by the CRL's Certification Advisory Panel who "ensures that the certification process addresses the interests of the entire CRL community, and includes leaders in collection development, preservation, and information technology."[30]

External audits against ISO 16363 and DIN 31644 will also be fee-based, but there is no current practice available.

The cost quality management system certification with ISO 9001 and information security management system certification with ISO 27001 usually depends on the number of days the external auditor needs to spend visiting on site but for medium size organisations is likely to be in the range of € 50,000.

4.5 Audit and certification cost: value for money

Our data collection and analysis made it clear that detailed costing is seldom part of the initial work on audit, and benefits begin to accrue already from simple exploration and preparation for addressing the audited issues. Many of the processes involved in audit, for example records management improvement, business process analysis, overlap with other desirable business outcomes it is often impossible to identify such work as purely an investment for audit.

Practical experience and discussion with repository managers shows that each of these activities has different levels of costs associated with them dependent on a number of key factors:

- Standard applied
- Maturity of the organisation
- Size and structure of the organisation
- Control over policy and level of formal governance structures
- Trust of third parties
- Degree of outsourcing
- Degree of interoperability between organisations required
- Contractual obligations
- Rationale for applying the standard.

[29] http://www.langzeitarchivierung.de/Subsites/nestor/EN/nestor-Siegel/siegel_node.html
[30] http://www.crl.edu/archiving-preservation/digital-archives/portico-hathitrust/advisory-panel

5 Conclusions

This deliverable is part of a suite of case studies from work package 4 into indirect economic determinants that were analysed in deliverable D4.1 *A prioritised assessment of the indirect economic determinants of digital curation*. This report discussed costs and benefits of standards-based quality assurance that is associated with trustworthiness through audits and certification practice. Two further reports will look into risk assessment and business models as cost determinants (see the forthcoming D4.4 and D4.5).

With digital curation maturing as a discipline, the focus of applying standards in the domain has shifted from quality of products to quality of processes and is beginning to gradually move towards quality of competences and skills of people. Generally speaking, around 1994, the state of the art in digital preservation was mostly concerned with evaluating the quality of products, software and solutions. Efficiency and costs associated with equipment were, as a rule, direct, measurable costs, e.g. technology costs that could be planned and budgeted for. In 2014 the focus of the digital curation domain is on evaluating the quality of digital archive processes, workflows, information security and services. Quality is multi-dimensional or is very organisation-specific, i.e. dependent on the business model of the organisation and how digital preservation is embedded into the (core) business of the organisation. The associated investments into quality assurance of processes are, by definition, then also hard to measure and benchmark because quality is determined directly or indirectly by multiple overlapping cost factors (cf. D4.1 report). This report has selected just one cost factor in the longer quality assurance process—the evaluation of quality through audit and conferment of a trusted digital repository status through certification—and has demonstrated how difficult it is to extract costs directly related to this activity.

As the maturity of application of standards advances in digital curation, the state of the art in ten years' time will be related to assessing quality of skills and competences of repository staff. The competency levels that in 2014 are required on an abstract level and are fairly ill-defined in digital curation as a domain, will gather momentum over the coming years as a method of quality assurance in digital curation.

Section 2.3 above indicated a pattern of development of quality criteria and controls of digital curation through the regular review and updating of auditing standards. Standards concerned with establishing quality in a domain evolve towards establishing a formal framework for maintaining the quality in between audits that by their very nature can only evaluate a state captured as a snapshot in time. The International Organization for Standardization introduced the concept of a 'management system standard' (MSS) that provides a model to follow when setting up and operating a management system.[31] The MSS are defined for many areas where continual improvement of quality is expected—quality management, information security, risk management, records management, environmental management, etc. Digital curation can already benefit from the organisation applying these methods as they all contribute indirectly towards better quality and increased transparency of digital curation process. None of them can or will, however, offer direct control and benchmarking for digital curation actions like the current generation of trusted digital repository auditing checklists do. For the digital repository audit standards to offer mechanisms for ensuring continual quality improvement that can be formally certified and trusted to last into the future, a management system would need to be established. The gap in the current standards-based quality assurance of digital repositories is illustrated in figure 1 below that compares the repository audit process with information security management audits:

[31] http://www.iso.org/iso/home/standards/management-standards.htm

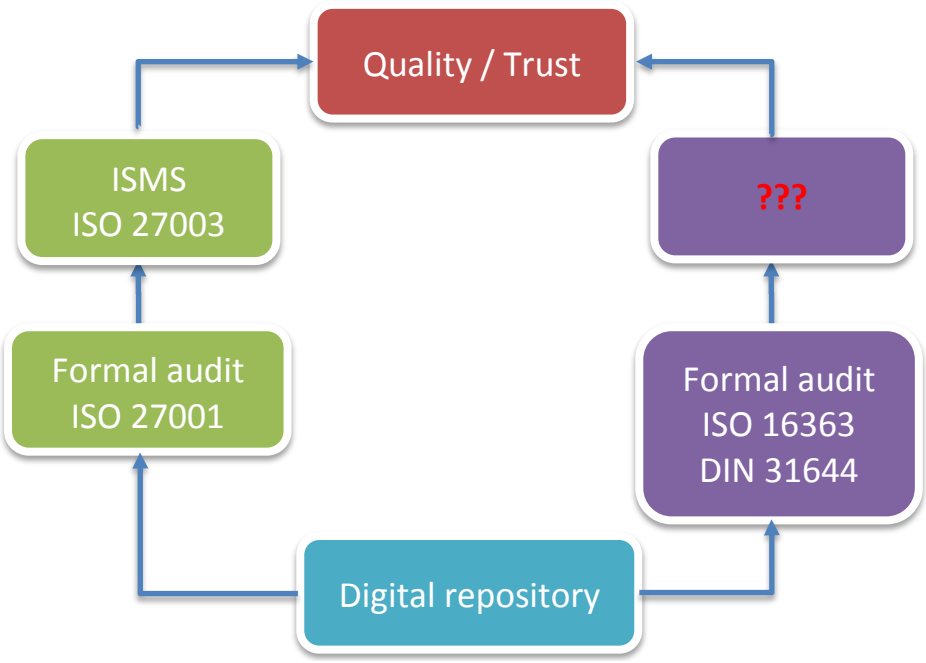

Figure 1—Digital repository audit standards compared with information security management system standards

Defining a management system for quality in digital curation would allow for better costing of curation activities through process or service level controls and also provide a mechanism for ensuring sustainability of the investments into the curation activity.

The reports from the digital curation community on the benefits of auditing and seeking certification testify that the primary motive at this stage is pragmatic—increased reputation and gaining competitive advantage on the market. Financial benefits through improved efficiency and quality of work are not the primary motives among repository managers.

5.1 Research funders' view

Members of the 4C project advisory board representing funding organisations (with responsibility for data archives) were invited to participate in a focus group to discuss trust and quality related costs. The focus group discussed the following questions:

- What is a trusted digital repository? Or what are trusted digital curation services?
- How important is trust in the opinion of funding organisations?
- Whose responsibility is it to measure trust?
- How could a funder measure trust? Are there other measures that could be applied?
- Can you express a figure / proportion of overall costs for TDR operations which should be applied to achieving trust?
- Are there known financial benefits (short term / long term) that accrue from repositories carrying out these activities?
- Is information security a special case?
- Should there be the same level of transparency in trust related activities as funders expect in research?
- What is the relationship between quality and trust?

Funding organisations represented were sceptical of the term 'trusted' digital repositories; there was a clear feeling that overall reputation and quality of service provision was more important than meeting the

requirements of a particular standard. Funders were interested in overall quality of service, which was not (in their terms) measured by existing standards. In effect our panel of funders were not interested in one standard another, they were only interested in ensuring that the feedback of *current* users demonstrated both quality and reputation of the repository. Of course repository managers will explain that the real users for whom they are carrying out these audit activities live well into the future, and that reputation is largely based on the past record of service.

There was general feeling that users would provide a level of control (via complaints to the funders) and that expert reviewers would also provide a level of control as part of a periodic review. Funders explicitly felt that there was no need for pre-emptive actions or regular checking of processes, except in particular circumstances.

Repository managers are less accepting that users and expert reviewers are able to provide an overall 'trust' perspective. Users, twenty years in the future may complain about the mis-curation of a digital object which renders it unusable, and the repository can do nothing about it. Similarly expert panels tend to focus on overall reputation and service delivery rather than the long term consequences of an action. In most cases reviews of repositories are carried out at either an organisational level or sub-organisational level and not at the 'curation' activity level. Typically these expert reviews are based on terms of reference constructed by the funding bodies without alluding to any of the 'standards' for trust.

In summary then, there appears to be a dichotomy between repositories aiming to achieve quality (and trust) on the level of curation processes, whereas the fund-makers are primarily interested in trust on the services level of the repository. (One funder stated: "No disasters is an easy measure of trust and reputation!")

Funders also had an overall feeling that the application of most 'standards' had internal applicability. It was summed up as meaning "that you managed to jump through the hoops and write down what you are doing." This misunderstanding of the application of trust standards is not confined to funders.

The general approach for national archives in this area is similar. There is an overwhelming focus on quality services and reputation, though the understanding of the desire to use standards-based assessment is more accepted, since these can be seen (though without much explicit evidence) to improve the service delivery (whether to internal or external customers). National archives may have a distinct approach to digital curation since they have a two-fold relationship with digital materials. First, they provide access to digital versions of material that they already curate on paper. Thus the acceptance of risk of loss of material is at a much lower level since it does not really matter much if these digital objects are lost. This attitude seems still to permeate to born-digital materials. Very few national archives have formal auditing or evaluation methods applied and digital curation still has not changed the main workflows of public archives. Consequently audit based approaches to reputation management and quality control are less applicable.

5.2 Conclusions for on-going 4C work

The Economic Sustainability Reference Model (ESRM) is a resource that has been supported and progressed by the 4C project and has been made available in draft form for community comment on the 4C website.[32] The purpose of this model is to set out a framework for designing a sustainability strategy for digital assets and services and it is clear that the issue of quality and trust is an integral concept for sustaining digital resources.

Quality assurance in digital curation is at the moment repository driven, in the sense that digital archives are responsible for selecting the best processes in relation to their particular business model. Whereas there is an expectation that quality is expressed and can be measured at the services level. In this situation, trust remains a latent variable in a digital repository, i.e., one that can intrinsically not be inferred from the measurements of observable variables.

Recommendation 1:

The ESRM should acknowledge that trust is presently a latent variable in a digital repository context; but that in the future it would be hoped that it would become more measurable, so its direct costs could be measured.

Transparency can increase reputation of a digital repository at minimal cost and is seen by many as a benefit. Formal auditing methods are perceived as being costly and presently less rewarding in terms of establishing trust than the openness that is achieved through publishing the results of a self-assessment or risk assessment.

Recommendation 2:

The ESRM should promote the concept of transparency around costs as a cost-effective way of increasing the reputation of the repository in the eyes of the key stakeholders.

Recommendation 3:

The ESRM should also recognise that reputation cannot easily be monetised, either in its cost or in its value. Similarly achieving a "comfortable" level of trustworthiness is dependent on the mission of the organisation, the risk appetite of that organisation, and other factors.

Calculating the cost of audit is at present perceived as high cost, difficult and not hugely beneficial since the costs incurred by one organisation will almost certainly not be comparable with another. Audit costs may not be easy to distinguish from on-going operational costs. An example of difficulty with audit costs is the implementation of audit results or to meet quality criteria. Altering a policy in an organisation to meet the requirements of a standard may take a few hours; implementing that policy may take a week or a month or a year; and ensuring that all relevant staff understand it and can implement it in their day-to-day tasks may take years. (These times are all elapsed times). As most cost methodologies are based on some form of (individual) Activity Based Costing, how is the staff member able to decide whether the implementation of a policy is a continued part of the audit/certification process or simply one of their ongoing job-related tasks. This difficulty has contributed to the low response rate this task has achieved to its call for sharing audit cost data.

[32] http://4cproject.eu/community-resources/outputs-and-deliverables/ms9-draft-economic-sustainability-reference-model

Recommendation 4:

As part of establishing an understanding of 'processes' (one of the ESRM 'key entities'), one of the processes that should be tracked at the time at which it takes place is the cost of certification because of the impracticality of retrospectively establishing it. The audit process as a specific (named) process in the ESRM should be removed and these costs included in the cost of 'carrying out operations' which, depending on the mandate of the repository may (or may not) include audit practices.

References

APARSEN (2012). D33.1B *Report on Peer Review of Digital Repositories*. http://www.alliancepermanentaccess.org/wp-content/uploads/downloads/2012/04/APARSEN-REP-D33_1B-01-1_1.pdf

APARSEN (2013a). D32.1 *Report on Cost Parameters for Digital Repositories*.

APARSEN (2013b). D32.2 *Report on Testing of Cost Models and Further Analysis of Cost Parameters*.

Ambacher, Bruce (2007). *Government Archives and the Digital Repository Audit Checklist*. In: Journal of Digital Information. Vol. 8(2) http://journals.tdl.org/jodi/article/view/190/171

Bechard, L., Massol, M. (2012) *Quality and accreditation in a French digital repository*. Paper presented at ICA 2012, 20-24-August 2012, Brisbane. http://ica2012.ica.org/files/pdf/Full%20papers%20upload/ica12Final00119.pdf

CCSDS (2011). *Audit and Certification of Trustworthy Digital Repositories. Recommendation for Space Data System Practices*. CCSDS 652.0-M-1. Magenta Book. Issue 1. Washington, D.C.

CPA/RLG (1996). *Preserving Digital Information: Report of the Task Force on Archiving of Digital Information*

Dallmeier-Tiessen S., Darby R., Gitmans K., Lambert S., Suhonen J., Wilson M. (2012). *Compilation of Results on Drivers and Barriers and New Opportunities*. http://www.alliancepermanentaccess.org/wp-content/uploads/downloads/2012/08/ODE-CompilationResultsDriversBarriersNewOpportunities1.pdf

Data Seal of Approval http://datasealofapproval.org/en/

DCC (2009). *The DCC Curation Lifecycle Model* http://www.dcc.ac.uk/sites/default/files/documents/publications/DCCLifecycle.pdf

Debenham, J., Sierra, C. (2008). *A Map of Trust between Trading Partners*. In: Furnell, S.M., Katsikas, S.K., Lioy, A. (Eds.), *TrustBus 2008.* LNCS 5185. Springer-Verlag. pp. 8-17

DELOS (2007). *A Reference Model for Digital Library Management Systems* http://delos.info/index.php?option=com_content&task=view&id=345&Itemid=

DIN 31644:2012 *Information und Dokumentation - Kriterien für vertrauenswürdige digitale Langzeitarchive*

DL.org (2011). *DL.org Reference Model* http://www.dlorg.eu/index.php/outcomes/reference-modeloutcomes/reference-model

Dobratz, S., Rödig, P., Borghoff, U.M., Rätzke, B., Schoger, A. (2010). *The Use of Quality Management Standards in Trustworthy Digital Archives*. In: The International Journal of Digital Curation. Vol. 5 (1) 46-63

DRAMBORA - Digital Repository Audit Method Based on Risk Assessment http://www.repositoryaudit.eu/

ERPANET (2004). *The Role of Audit and Certification in Digital Preservation*. Final report of the erpaWorkshop in Antwerp http://www.erpanet.org/events/2004/antwerpen/Workshop_Antwerpen_report.pdf

European Framework for Audit and Certification of Digital Repositories (2010) http://www.trusteddigitalrepository.eu/Site/Trusted%20Digital%20Repository.html

Harmsen, Henk (2008). *Data seal of approval - assessment and review of the quality of operations for research data repositories*. In: *Proceedings of the iPRES 2008 Conference*. British Library

Hofman, H., McHugh, A., Ross, S., Ruusalepp, R. (2007). *Digital Repository Audit Method Based on Risk Assessment* http://www.repositoryaudit.eu/downloadDRAMBORA

InterPARES (2007). *Chain of Preservation (COP) Model* http://www.interpares.org/ip2/ip2_models.cfm#

ISO (2012). *Quality management principles* http://www.iso.org/iso/qmp_2012.pdf

ISO 14641-1:2012 *Electronic archiving — Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation*

ISO 14721:2012 *Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model*

ISO 16363:2012 *Space data and information transfer systems -- Audit and certification of trustworthy digital repositories*

ISO/DIS 16919 *Space data and information transfer systems - Requirements for bodies providing audit and certification of candidate trustworthy digital repositories*

ISO/IEC 17021:2011 *Conformity assessment – Requirements for bodies providing audit and certification of management systems*

ISO/TR 17068:2012 *Information and documentation — Records management — Trusted third party repository for digital records*

ISO/IEC 27002:2013 *Information technology – Security techniques – Code of practice for information security controls*

Li, W., Ping, L. (2009). *Trust Model to Enhance Security and Interoperability of Cloud Environment*. In: Jaatun, M.G., Zhao, G., Rong, C. (Eds.) Cloud Computing. Springer-Verlag. pp. 69-79

McHugh, A., Ross, S., Innocenti, P., Hofman, H., Ruusalepp, R. (2008) *Bringing Self-assessment Home: Repository Profiling and Key Lines of Enquiry within DRAMBORA*. In: International Journal of Digital Curation, Vol. 3(2) http://www.ijdc.net/index.php/ijdc/article/view/93/64

Massol, M, O. Rouchon, L. Bechard, (2011) *Certification and Quality: A French Experience*, paper given at iPRES2011, 1-4 November 2011, Singapore.

nestor (2006) *Criteria for Trusted Digital Long-Term Preservation Repositories - Version 1* (Request for Public Comment), edited by nestor - Network of Expertise in Long-Term Storage of Digital Resources and nestor Working Group on Trusted Repositories Certification. nestor materials 8 http://nbn-resolving.de/urn:nbn:de:0008-2006060703

nestor (2008). *nestor-Kriterien: Kriterienkatalog vertrauenswürdige digitale Langzeitarchive*. Kompetenznetzwerk Langzeitarchivierung / Arbeitsgruppe Vertrauenswürdige Archive – Zertifizierung. Version 2 http://www.nbn-resolving.de?urn:nbn:de:0008-2008021802

nestor (2013). *Explanatory notes on the nestor Seal for Trustworthy Digital Archives*. nestor Certification Working Group. nestor-materials 17 http://files.d-nb.de/nestor/materialien/nestor_mat_17_eng.pdf

OCLC/RLG (2007). *Trustworthy Repository Audit and Certification (TRAC): Criteria and Checklist* http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf

Palaiologk, A. S., Economides, A. A., Tjalsma, H. D. & Sesink, L. B. (2012). *An activity-based costing model for long-term preservation and dissemination of digital research data: the case of DANS*. In: International Journal on Digital Libraries. Vol. 12 (4), pp 195-214. http://link.springer.com/article/10.1007%2Fs00799-012-0092-1

RLG/OCLC (2002). *Trusted Digital Repositories: Attributes and Responsibilities.* http://www.oclc.org/research/activities/past/rlg/trustedrep/repositories.pdf

Rotter, J. B., *A New Scale for the Measurement of Interpersonal Trust* // Journal of Personality, Vol. 35, 1967, pp. 651-665

Ruusalepp, R., Lee, C.A., van der Werf, B., Woollard, M. (2012). *Standards Alignment*. In: McGovern, N.Y., Skinner, K. (Eds.). Aligning National Approaches to Digital Preservation. pp. 115-166. Atlanta: Educopia Institute Publications

Salo, J., Karjaluoto, H. (2007). *A conceptual model of trust in the online environment*. In: Online Information Review. Vol. 31(5) 604-621

Shekarpour, S., Katebi, S.D. (2010). *Modeling and evaluation of trust with an extension in semantic web*. In: Web Semantics: Science, Services and Agents on the World Wide Web. Vol. 8. 26–36.

Annex 1: Questionnaire

About yourself
Name of the organization
Organization type (e.g. memory institution, vendor, service provider, research institutions, etc.)
Type of audit or certification (e.g. ISO, national, domain, institutional)
Audit / certification details (including time, period, location, number of people involved, etc.)
Motivation for audit/certification or target set by the organization
Time taken to prepare for audit / certification
Final certification date
Estimated total cost of preparing for audit/certification
Estimated total cost of actual obtaining of the certificate
Main resources that were required for conducting audit/certification at your organization (e.g., people, materials)
Lessons learned from the audit / certification
Expected benefits of the audit / certification and did it represent good return on investment?
Overall evaluation of the certification effort

What were the resources needed for the audit/certification?		
Resources	**Cost**	**Time**
Internal staff		
External staff (consultants)		
Equipment		
Hardware		
Software		

How much did the preparation of audit/certification cost?		
Activity	**Cost**	**Time**
Preparation of evidence/documentation		
Creating / updating the asset inventory		
Interviews with staff		
Assessing level of conformance to the standard		
Creation of new evidence if it does not already exist		
Risk assessment		

How much did you spend on re-arranging policies/procedures prior to the audit?		
Activity	**Cost**	**Time**
Changing policy/procedures if the procedures do not meet the standard		
Implementing policy/procedures		

How much did the actual audit/certification process cost?		
Activity	**Cost**	**Time**
Analysis of evidence and producing the evidence		
Interviews and discussions		
On-site audit/certification support		
Follow-up activities after the on-site visit		

Other
What kind of expenses did you have to make after the audit/certification process was over? (e.g. for adjusting your practices and policies)
What are the costs of maintaining the certification? (including the costs of maintaining the evidence base and documentation for follow-up audits)
Were there any additional costs?
Any other comments or suggestions for an auditing cost model or for the 4C project?

Annex 2: Summary of literature review on audit and certification practice

A2.1 Audit and certification experience

Parameter	Information
Source (Paper, Article, etc.)	Presentation that summarizes the lessons learned from a set of audits of several production distributed digital preservation networks and suggest a coordination of efforts to develop standardized auditing tools to implement the ISO audit standards and other standards.
Name of the organization	
Organization Profile	
Type of Certification (e.g. ISO, national, domain, institutional)	ISO audit standards and other standards such as the Data Seal of Approval.
Certification details	
Motivation for certification	
Time to complete certification	In this study was analysed the operation of networks over the course of 24 months.
Final certification date	
Cost of preparing for certification	
Cost of actual certificate	
Resources needed for certification (i.e. people, materials)	These audits were conducted using the open source SafeArchive system.
Lessons learned	The analysis of the audit yields a number of lessons for improving Distributed Digital Preservation implementation and underscores the importance of periodic, automated policy audits. The use of DDP's significantly reduces content risk
Expected benefits of certification	The analysis of networks allowed joining about 1200 collections of content, hosted by more than 30 institutions. The audit yielded surprising results.
Return on Investment	This study shows that standardized audits are valuable tools and as Distributed Digital Preservation become more international; in scope the development of audit tools that meet the joint needs of the international community will be required.
Overall evaluation of the certification effort	An analysis of the trial audits demonstrates both the complexities of auditing modern replicated storage networks, and reveals common gaps between archival policy and practice.

Parameter	Information
Source (Paper, Article, etc.)	Document that shares the experience of certified Portico as a trustworthy digital repository, by Amy Kirchhoff, Eileen Fenton, Stephanie Orphan and Sheila Morrissey
Name of the organization	Portico preservation service
Organization Profile	Portico is a not-for-profit digital preservation service that provides a permanent archive of electronic journals, books, and other scholarly content. This service belongs to ITHAKA, a not-for-profit organization dedicated to help the academic community
Type of Certification (e.g. ISO, national, domain, institutional)	Trustworthy Digital Repository
Certification details	This certification is subdivided in three categories: • Organizational infrastructure; • Digital object management; • Technologies, technical infrastructure, and security The audit process was based on the Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC), as well as other inputs of interest to the CRL community.
Motivation for certification	One method for these digital repositories to assure themselves and their communities of their soundness is to be audited and certified by impartial organizations.
Time to complete certification	Portico was involved in audit preparation and the actual audit for approximately 16 months (from the fall of 2008 until January 2010), although the audit itself extended over 10 months.
Final certification date	The audit was formally concluded in January 2010, when CRL certified Portico as a trustworthy digital repository.
Cost of preparing for certification	The preparation for the audit included a process of collecting and updating documentation in order to make it easier to provide the documentation to other parties subsequently to the audit. This documentation was organized into 5 portfolios: • Organization; • Policy; • System Architecture and Content Model; • Operations and Systems Development & Maintenance; • Archive Interfaces
Cost of actual certificate	To maintain the Portico's credibility, Portico will provide CRL with updated documentation every two years and will continue dialogue with CRL on the main priorities

Parameter	Information
Resources needed for certification (i.e. people, materials)	From the CRL audit team, it was necessary two full-time CRL staff members and one CRL technical consultant. The principal human resources of Portico archive was composed by a product manager, Amy Kirchhoff, senior research developer, Sheila Morrissey, publisher content coordinator, Stephanie Orphan. It is important to refer that many staff of Portico participated, including staff from library outreach, publisher outreach, legal, finance, user services, operations, and development. Beyond human resources, it was necessary some materials like documentation from a variety of Departments.
Lessons learned	With the CRL report and all preparation to the audit, Portico understood that exist some documentation discrepancies. Nevertheless, Portico has already addressed some issues identified in the CRL report.
Expected benefits of certification	One substantial benefit from this process is simply the opportunity for external review and validation of the approach and processes employed by Portico in pursuit of their preservation of work. Furthermore, Portico frequently interacts with members of the community and responds to requests for information. Another benefit arose from the CRL audit team's interest in speaking with a Portico data export partner. The greatest benefit to Portico was simply the reassurance to Portico and the ITHAKA Board, to the publisher community, to the library community, and to the greater academic community, that the Portico archive was being rigorously examined by an external party.
Return on Investment	The most significant benefit is the assurance regarding the viability, the integrity, and the effectiveness of Portico's preservation approach that only such a comprehensive, objective, third-party review can provide.
Overall evaluation of the certification effort	It is difficult to measure the impact of the certification, but at the end, the process served Portico well. For example, Portico's certification has been a point of conversation with the National Library of Medicine.

Parameter	Information
Source (Paper, Article, etc.)	Document that shares the experience and opinion to elaborate a data seal of approval in order to become a trusted digital repository by Dr. Henk Harmsen
Name of the organization	Data Archiving & Networked Services
Organization Profile	The organization is active in the area of data infrastructure, with two main themes, namely (digital) archiving and making research data available. The field of activity of DANS covers both the social sciences and the humanities.
Type of Certification (e.g. ISO, national, domain, institutional)	Elaboration of data seal of approval by DANS to become a Trusted Digital Repository. (TDR)
Certification details	To be a trusted digital repository the organization made a data seal of approval that consists on 17 guidelines that may be helpful to an archiving institution striving to become a trusted digital repository (TDR). This data seal of approval expresses the provisions that an archive has been made to guarantee the safety and future usability of the data.
Motivation for certification	The motivation for certification was to encourage the idea of shared responsibility and be a trustful organization.
Time to complete certification	
Final certification date	
Cost of preparing for certification	
Cost of actual certificate	
Resources needed for certification (i.e. people, materials)	There are 4 stakeholders for the seal of approval: • The financial sponsor • The data producer • The data consumer • The data repository Further the resources given, it was necessary information about organization, like processes and technical infrastructure.
Lessons learned	The objective of the data seal of approval was mainly to try and convince archiving institutions to start paying attention to quality management.
Expected benefits of certification	The DSA offers possibilities for subcontracting archiving and still meet the requirements of the DSA. Research groups with their own data projects will appreciate this.
Return on Investment	The elaboration of DSA is not in conflict with for example TRAC, but is rather a step toward it.
Overall evaluation of the certification effort	DANS strives toward internationalization of the data seal of approval. The previously mentioned DSA assessment group will be launched in the fall of 2008, and that same year, four pilots will be planned in The Netherlands as a first step in the area of certification of the DSA.

Parameter	Information
Source (Paper, Article, etc.)	Article that relates an experience on quality and accreditation in a French digital repository, by Lorène BECHARD and Marion MASSOL
Name of the organization	CINES (Centre Informatique National de l'Enseignement Supérieur)
Organization Profile	CINES is a state administration institution based in Montpellier (France) which employs about 50 engineers and which is known worldwide for its HPC (high performance computing) activities. Their infrastructures are available for all French researchers, who are split up into scientific domains. The largest communities to use the CINES computing services are the fluid mechanics, chemistry and climatology research communities.
Type of Certification (e.g. ISO, national, domain, institutional)	The CINES strategy encompassed the improvement of the quality of the service provided based on various standards like: • ISO 14 721 (Open Archival Information System); • ISO 16 363 ("audit and certification of trustworthy digital repositories"); • ISO 16 919 ("requirements for bodies providing audit and certification of candidate trustworthy digital repositories"); • AFNOR NF Z42-013 (French recommendations about conception and utilization of systems with data to preserve, now is called ISO 14641-1), • PAIMAS (Producer-Archive Interface Methodology Abstract Standard), • SEDA – a French standard about archives exchanges (Standard d'Echange de Données pour l'Archivage), • P2A - Politique et pratiques d'archivage (policy and practices about preservation in a French public environment • DSA - Data Seal of Approval • DRAMBORA - Digital Repository Audit Method Based on Risk Assessment • TRAC - Trustworthy Repositories Audit & Certification (TRAC): criteria and checklist
Certification details	ISO 14721 & NF Z42-013 –This certification allows organizations to store and preserve on the national territory some public records (non-heritage) provided that they have received an authorization from SIAF (Service Interministériel des Archives de France). ISO 16363 –This framework wants to federate the different accreditation and certification project into three levels of recognition of the quality assurance effort done by institutions in charge of the preservation of the digital heritage, in increasing trustworthiness DSA –This seal is granted to the digital preservation centers, for establishing quality assurance procedures to ensure accessibility and intelligibility of information entrusted to them DRAMBORA–it allows the identification and classification risks that could impact the proper performance of its service

Parameter	Information
Motivation for certification	ISO 14721 & NF Z42-013 –CINES consider that preserve data over time requires the implementation of a rigorous quality assurance approach, in order to manage and mitigate the risks associated to this activity. As a public institution, and given the need expressed by its community, decided to position itself on this sector. ISO 16363 –The motivation for this certification was to obtain the most relevant certification from the perspective of the funding bodies. DRAMBORA—The aim here is not to eliminate the risks, but to determine acceptable levels of risk and mitigate them before damage occurs.
Time to complete certification	ISO 14721 & NF Z42-013 –According to the document, takes as long as 6 months ISO 16363– Takes as long as 3 years DSA—Takes as long as 2 years
Final certification date	ISO 14721 & NF Z42-013– Has a period of three years counting of the date that is approved.
Cost of preparing for certification	ISO 14721 & NF Z42-013 – The requirements for obtain this certification consist of twenty-two technical, operational, organizational, strategic and legal criteria
Cost of actual certificate	
Resources needed for certification (i.e. people, materials)	ISO 14721 & NF Z42-013 – To obtain this certificate, it was necessary that experts from SIAF visited the CINES facilities and interviewed its representatives to verify if the twenty-two technical, operational, organisational, strategic and legal criteria was implemented. ISO 16363 – The resources for this certification was distributed in two parts: • External: analysis of the reference document, definition of the scope of the audit, preparation of the main deliverable – report document in French, planning) • Internal: evaluation and documentation of the criteria fulfilment in French, translation of the report in English language, additional interviews and verifications, gap analysis with the 2009 external audit report. DSA – CINES had to submit a request on the web that consists of a self-assessment of the sixteen Data Seal of Approval guidelines.
Lessons learned	ISO 14721 & NF Z42-013 –To renewal the certificate, SIAF provided a list of conditions and recommendations, that CINES has already taken them into account in a specific action plan. ISO 16363 – the auditors expressed remarks and recommendations for CINES to improve the quality of the services provided, where necessary. DRAMBORA – thirty-eight main risks have been identified and defined from the seventy-eight risks listed in DRAMBORA.
Expected benefits of certification	ISO 16363 – CINES is waiting for the release of an associated standard (ISO/DIS 16919) that will enable auditors' certification, so that they are able to certify repositories in return, on the basis of the ISO 16363.
Return on Investment	ISO 16363—covers exactly the scope of PAC activities along with the visibility of an ISO standard. DRAMBORA—In the particular case of the PAC service, the risk management plan was established in 2009 and is still reviewed every six months by the whole team.

Parameter	Information
Overall evaluation of the certification effort	A quality assurance approach based on certification prerequisites can be a guide for those who wish to establish a long-term digital preservation service. By providing a list of requirements, a certification frame of reference can help to the drafting of specifications. It recognizes its quality and professionalism, and therefore establishes trust with communities of users, and potentially leverages budgets from funding bodies.

Parameter	Information
Source (Paper, Article, etc.)	Document that shares the experience of certified Chronopolis as a trustworthy digital preservation network, by Marie Waltz and other CRL staff.
Name of the organization	Chronopolis digital preservation network.
Organization Profile	Originally funded by the Library of Congress, the Chronopolis digital preservation network has the capacity to preserve hundreds of terabytes of digital data—data of any type or size, with minimal requirements on the data provider. Chronopolis comprises several partner organizations that provide a wide range of services. The partners include: • San Diego Supercomputer Center (SDSC) at UC San Diego; • UC San Diego Libraries (UCSDL); • National Center for Atmospheric Research (NCAR); • University of Maryland Institute for Advanced Computer Studies (UMIACS).
Type of Certification (e.g. ISO, national, domain, institutional)	Trusted Digital Repository (TRD).
Certification details	This certification is subdivided in three categories: • Organizational Infrastructure; • Digital object management; • Infrastructure and Security Risk Management. The audit process was based on the Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC), as well as other inputs of interest to the CRL community. The audit used also as reference the Open Archive Information System reference model (OAIS).
Motivation for certification	CRL certification applies specifically to the repository's ability to preserve and manage digital files and data deposited by the Inter-university Consortium for Political and Social Research; and diverse sets of data files from the California Digital Library, North Carolina Geospatial Data Archiving Project, and the Scripps Institution of Oceanography. CRL did not assess Chronopolis procedures and processes for normalizing, migrating, or otherwise altering and preserving data for distribution via future platforms or devices.
Time to complete certification	Chronopolis preservation audit occurred for approximately 14 months (from November 2010 until December 2011).
Final certification date	The audit formally concluded in December 2011, when CRL certified Chronopolis as a trustworthy digital repository.

Parameter	Information
Cost of preparing for certification	The preparation for the audit included a process of collecting and updating documentation in order to make it easy to provide the documentation to other parties subsequent to the audit. This documentation was organized into 4 portfolios: • Funding Plan and Financial Benchmarks; • Preservation Policies and Tools; • Digital Curation; • Business and management plans.
Cost of actual certificate	To retain trusted status, a repository will need to undertake a regular cycle of audit and/or certification. To that end CRL and Chronopolis have agreed that on-going certification is contingent upon Chronopolis to provide CRL with updated documentation every two years and will continue dialogue with CRL on the main priorities.
Resources needed for certification (i.e. people, materials)	CRL analysis of Chronopolis documentation and operations was undertaken by Marie Waltz and other CRL staff. Additional technical support for the site visit and the assessment of Chronopolis repository systems and architecture was provided by Ann Green of Digital Life Cycle Research & Consulting. From Chronopolis, it was necessary information from the partners: UC San Diego Supercomputer Center, David Minor and Don Sutton; UC San Diego Libraries, Ardys Kozbial; National Center for Atmospheric Research, Michael Burek; University of Maryland Institute for Advanced Computer Studies, Michael Smorul. This certification is based upon review by CRL and the members of its Certification Advisory Panel of extensive documentation gathered by CRL independently from open and third-party sources as well as data and documentation provided by Chronopolis.
Lessons learned	Chronopolis is strong on technology but not so good on business plans. It should take in consideration the elaboration of good data on costs and plans and needs a better projection for the future – long-term preservation plan and a correct definition of the designed communities.
Expected benefits of certification	Implement recommendations by better identifying new users and communities, improving the work with other networks, make management plans and adopt long-term preservation strategies.
Return on Investment	The most significant benefits are: to do a validation of work so far, learn about holes, hear community comments, and increase business.

Parameter	Information
Overall evaluation of the certification effort	The overall conclusion of the panel was that Chronopolis could be recognized by the designated community as a trustworthy repository with certain important considerations. One consideration is the level of preservation service Chronopolis provides. The repository's mission statement identifies Chronopolis' goal as providing "a preservation data grid and its supporting human, policy, and technological infrastructure." However, Chronopolis does not commit to services beyond preserving intact the bits deposited in the repository. This limitation is clearly expressed in the Chronopolis subscriber license agreement, which disclaims responsibility for performing specific "preservation actions" that some other repositories provide, such as format migration, file normalization, file type verification, and creation of descriptive metadata. Because this limitation is clearly communicated to Chronopolis stakeholders, Chronopolis can be said to provide preservation services adequate to its community. The second consideration is Chronopolis' relatively nascent and untested administrative infrastructure and business plan. At the time of this review Chronopolis was transitioning from being a largely grant-supported project to a university-based service that is expected to provide digital storage for research data in a variety of fields on a fee-for service basis. Chronopolis had also established strong partnerships with the organizations hosting its three modules, and has secured commitments from those organizations to cover their own respective costs for the next several years.

Parameter	Information
Source (Paper, Article, etc.)	Document that shares the experience of certified Scholars as a trustworthy digital repository, by Marie Waltz and other CRL staff.
Name of the organization	Scholars Portal digital repository service.
Organization Profile	Scholars Portal (www.scholarsportal.info/) was created in 2002, as a repository for digital content licensed, purchased, and otherwise acquired by the 21 Canadian libraries represented by the Ontario Council of University Libraries (OCUL) consortium. Scholars Portal provides a common technical infrastructure for delivering digital content and services to support research, teaching, and learning within the Ontario higher education community. Scholars Portal was initially created as a local hosting solution for licensed content. It has since evolved to include digital preservation, archiving, and repository services.
Type of Certification (e.g. ISO, national, domain, institutional)	Trusted Digital Repository (TRD).
Certification details	This certification is subdivided in three categories: • Organizational Infrastructure; • Digital object management; • Infrastructure and Security Risk Management. The audit process was based on the Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC), as well as other inputs of interest to the CRL community. The audit used also as reference the Open Archive Information System reference model (OAIS) and the standard ISO 16363.
Motivation for certification	This assessment was undertaken to determine whether the Scholars Portal e-journals archive meets the commitments the repository's management has made to its stakeholders with regard to the long-term preservation of e-journals for the academic research community, and whether the repository complies with established criteria for trusted digital repositories.
Time to complete certification	Scholars Portal was involved in audit preparation and the actual audit for approximately 6 months (from January 15 until July 15, 2012).
Final certification date	The audit formally concluded in July 2012, when CRL certified Scholars as a trustworthy digital repository.

Parameter	Information
Cost of preparing for certification	The preparation for the audit included a process of collecting and updating documentation in order to make it easy to provide the documentation to other parties subsequent to the audit. This documentation was organized into 8 portfolios: • Succession Planning; • Procedural Accountability and Policy Framework; • Monitoring Integrity of Archival Objects; • Technical Infrastructure Risk Management; • Backups and Disaster Recovery; • Preservation Planning; • Access Management; • Information Management.
Cost of actual certificate	To retain trusted status, a repository will need to undertake a regular cycle of audit and/or certification. To that end CRL and Scholars Portal have agreed that on-going certification is contingent upon Scholars Portal to provide CRL with updated documentation every three years and will continue dialogue with CRL on the main priorities.
Resources needed for certification (i.e. people, materials)	From the CRL audit team, it was necessary one full-time CRL staff member and other CRL staff members, as well as one CRL technical consultant. From the Scholars Portal, it was composed by Caitlin Tillman OCUL IR Chair, Caitlin Tillman, OCUL Executive Director, Kathy Scardellato, as well as the participation of other OCUL member institutions.
Lessons learned	Scholars Portal acknowledges that implementation of an online mirror site would provide an additional layer of security and ensure continuous service in the event of a disaster and that mirroring would provide online redundancy of archival storage, data management, and dissemination systems. Consequently, at the time of this report Scholars Portal and its administrators, the Ontario Council of University Libraries, were endeavouring to engage another entity to take on the role of a mirror site and CRL encourages them to continue this activity.
Expected benefits of certification	One substantial benefit from this process is simply the opportunity for external review and validation of the approach and processes employed by Scholars Portal in pursuit of their preservation work. Furthermore, Scholars Portal frequently interacts with members of the community and responds to requests for information.
Return on Investment	The most significant benefit is the assurance regarding the Authenticity, the Integrity, and the Usability of Scholars Portal preservation approach that only such a comprehensive, objective, third-party review can provide.
Overall evaluation of the certification effort	The certification of Scholars Portal provided accountability, the collection of stewardship and helped establishing and stimulated discussions of digital preservation in Canada.

Parameter	Information
Source (Paper, Article, etc.)	Document that shares the information of the use of DRAMBORA as a trustworthy digital repository audit method based on risk assessment, by Andrew McHugh, Sarah Jones, Joy Davidson, Seamus Ross.
Name of the organization	DRAMBORA (Digital Repository Audit Method Based On Risk Assessment).
Organization Profile	Developed jointly by the Digital Curation Centre (DCC) and Digital Preservation Europe (DPE), the Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) represents the main intellectual outcome of a period of pilot repository audits undertaken by the DCC throughout 2006 and 2007. It presents a methodology for self-assessment, encouraging organizations to establish a comprehensive self-awareness of their objectives, activities and assets before identifying, assessing and managing the risks implicit within their organization. Within DRAMBORA, digital curation is characterized as a risk-management activity; the job of a digital curator is to rationalize the uncertainties and threats that inhibit efforts to maintain digital object authenticity and understandability, transforming them into manageable risks.
Type of Certification (e.g. ISO, national, domain, institutional)	Digital Repository Audit Method Based On Risk Assessment.
Certification details	Within DRAMBORA, digital curation is characterized as a risk-management activity; the job of a digital curator is to rationalize the uncertainties and threats that inhibit efforts to maintain digital object authenticity and understandability, transforming them into manageable risks. Six stages are implicit within the process. Initial stages require auditors to develop an organizational profile, describing and documenting the repository's mandate, objectives, activities and assets. Latterly, risks are derived from each of these, and assessed in terms of their likelihood and potential impact. Finally, auditors are encouraged to conceive of appropriate risk management responses to the identified risk. The process enables effective resource allocation, enabling repository administrators to identify and categorize the areas where shortcomings are most evident or have the greatest potential for disruption. The process itself is an iterative one, and therefore subsequent recursions will evaluate the effectiveness of prior risk management implementations.
Motivation for certification	DRAMBORA enables organizations to better fulfil their responsibilities and achieve their strategic goals by identifying the strengths and weaknesses of their digital repository, and assisting them to plan effectively to mitigate these risks.
Time to complete certification	It is anticipated that the self-audit process will take approximately 24-30 hours (or, at six hours per day, four to five days). Each individual task is allocated an estimated effort requirement, although, depending upon the scale and scope of repository operations, and the degree of scrutiny with which the assessment is conducted, this may vary, occasionally substantially.
Final certification date	In reality, the core activity, the conception and management of an organizational risk register, is something that is never finalized, and requires reassessment over time to ensure its on-going relevance and applicability.

Parameter	Information
Cost of preparing for certification	Before beginning the assessment, it is necessary a preliminary analysis of the repository documentation, and arrange appointments with repository staff for onsite interviews and visits to the repository site. The Drambora workflow follows the next structure: • Define Audit Purpose and Scope; • Formalize Staffing and Roles; • Determine Functional Classes; • Formalize Mandate(s); • Formalize Constraints; • Formalize Objectives; • Formalize Activities and Assets; • Identify Risks; • Assess Risks; • Manage Risks.
Cost of actual certificate	After completing the assessment, the are two distinct outputs: a risk register of the repository, produced using the automatic DRAMBORA reporting system; an audit report structured along the ten characteristics of digital preservation repositories: • Mandate & Commitment to Digital Object; • Maintenance; • Organizational Fitness; • Legal & Regulatory Legitimacy; • Efficient & Effective Policies; • Adequate Technical Infrastructure; • Acquisition & Ingest; • Preservation of Digital Object Integrity; • Authenticity & Usability; • Metadata Management & Audit Trails; • Dissemination; • Preservation Planning & Action. This report is produced using the documentation and information collected and analysed for the assessment.

Parameter	Information
Resources needed for certification (i.e. people, materials)	The success of the audit process benefits from the participation in the process of key players within the organization. The primary auditor assumes responsibility for ensuring that all appropriate contributions from within the organization are solicited, obtained and appropriately assessed. In order for the process to be internally reliable, and for its outcomes to be regarded, as correct and complete, organizations should ensure that their auditors are both appropriately trained and have suitable personal skills. An auditor should have these main capabilities, based on ISO 19011 - guidelines for quality and/or environmental management systems auditing offers a good indication of the ideal characteristics an auditor should have and display: • high ethical standards; • open-mindedness; • diplomacy; • observational aptitude; • perceptiveness; • versatility; • tenaciousness; • decisiveness; • self-reliance.
Lessons learned	From the sample audits carried out, the lessons learned were: identified areas for future improvement in the DRAMBORA methodology; clarified key roles in the audit process; positive feedback received on direct and subsidiary benefits of carrying out audits.
Expected benefits of certification	Carrying out a DRAMBORA audit helps provide peace of mind with regard to growing, valuable and at-risk digital collections. It can strengthen the trust of users and staff, increase efficiency by helping to focus and refine operational policies, and may even highlight potential opportunities for repository managers to leverage increased development potential by offering a clear way to demonstrate the risks related to shortfalls in repository funding.
Return on Investment	Following the successful completion of the self-assessment exercise, organizations can expect to have: a well-established and documented organizational profile; clearly identified and documented repository assets, roles and activities; constructed a catalogue of pertinent risks and inter-risk relationships; developed a shared understanding of the successes and shortcomings of the repository's management and structure; alerted repository managers to the likelihood of a specific risk occurring; implemented contingency mechanisms to alleviate the effects of risks that cannot be avoided.
Overall evaluation of the certification effort	DRAMBORA enables internal assessment by providing repository administrators with a means to assess their capabilities, identify their weaknesses, and recognize their strengths.

Parameter	Information
Source (Paper, Article, etc.)	Article written by Robert R. Downs and Robert S. Chen that analyses the Self-Assessment of a Long-Term Archive for Interdisciplinary Scientific Data as a Trustworthy Digital Repository
Name of the organization	SEDAC—NASA Socioeconomic Data and Applications Center, operated by Center for International Earth Science Information Network (CIESIN) of Columbia University
Organization Profile	SEDAC –The main goal of this archive is to produce, archive, and disseminates scientific data and offers services to improve understanding of human interactions in the environment. According to National Science Board, SEDAC has been characterized as a "reference collection" serving "large segments of the general scientific and education community"
Type of Certification (e.g. ISO, national, domain, institutional)	SEDAC Long-Term Archive (LTA)
Certification details	SEDAC Long-Term Archive (LTA) – To evaluate alternative digital repository platforms, CIESIN is using the Open Source Software Suite Fedora as the basis for the LTA's digital repository and asset management system, in conjunction with the VITAL software from VTLS, Inc. If some of LTA board members decide to cease operations or lack the resources to maintain the archive, the Columbia Libraries have agreed to assume responsibility for the LTA as part of its own long-term digital repository. The LTA Board recommended a self-assessment of the LTA as an essential step. So, the TRAC document was chosen as the initial instrument for the self-assessment for several reasons, especially to conduct the self-assessment on a continuing basis to identify areas for further improvement and to check on past changes in processes and procedures.
Motivation for certification	SEDAC Long-Term Archive (LTA) – The principal motivation for this organization was to create an explicit responsibility for long-term archiving.
Time to complete certification	
Final certification date	
Cost of preparing for certification	
Cost of actual certificate	
Resources needed for certification (i.e. people, materials)	• the current technological infrastructure, • organizational capabilities, • relevant documentation • Nineteen resources categorized as policies, plans, procedures, forms, documentation, and contracts.

Parameter	Information
Lessons learned	Continuous assessment and improvements are needed to ensure that the trustworthiness of data and metadata are maintained as collections grow, as new technologies are adopted, and as new services are offered for current and future user communities.
Expected benefits of certification	Development of collaborations within and between institutions and associated contingency plans provides viable options for the long-term survivability of data and continued access.
Return on Investment	According to the article, the collective development of SEDAC LTA provides the basis for what they believe will be a sustainable organizational infrastructure for the archive, including both its technical infrastructure and the content of its collection.
Overall evaluation of the certification effort	The self-assessment of the SEDAC LTA has identified several important challenges and possible strategies for scientific data archives and repositories. Archives and repositories could benefit from continued self-assessment to ensure that they meet established criteria for trustworthiness, especially during the transition of infrastructure and collections to digital repository systems.

Parameter	Information
Source (Paper, Article, etc.)	Document that provide the experience that has been undertaken in support of the European Framework for Audit and Certification of Digital Repositories which was initiated by the European Commission's unit that funds APARSEN. In negotiation this work was integrated into the APARSEN project

Name of the organization	The organizations involved was:
	• Europe:
	  ○ Deutsche National Bibliothek (DNB)
	  ○ Koninklijke Nederlandse Akademie van Wetenschappen Data Archiving and Networked Services (DANS)
	  ○ UK Data Archive (UKDA)
	  ○ Centre Informatique National de l'Enseignement Supérieur: Département Archivage et Diffusion (CINES-DAD)
	• USA:
	  ○ Socioeconomic Data and Applications Center (SEDAC) at the Center for Earth Science Information
	  ○ National Space Science Data Center (NSSDC)
	  ○ Kentucky Department for Libraries and Archives (KDLA)

Organization Profile	
Type of Certification (e.g. ISO, national, domain, institutional)	• DSA (Data Seal of Approval) • ISO 16363 • DIN 31644
Certification details	DSA—The sixteen quality guidelines of the DSA are designed to support data producers, repositories and consumers in the reliable management of data for the future without requiring the implementation of new standards, regulations or high costs. There is no audit process or site visit: just a review on the basis of trust resulting in a clear, public statement of the process undertaken. ISO 16363 – was designed to form the basis for a full external audit process of all types of repositories, from cultural to science to commercial, and with international, trained, consistent, cohorts of auditors to supply whatever the scale of demand. The creation process of this standard as an important part that it was the creation of a second standard. It means that, was created another certificate, called ISO/DIS 16919 which defines the way in which the external audit and certification must be undertaken, following and specializing the ISO hierarchy of standards defining audit processes. DIN 31644 –This standard comprises an introduction addressing the challenges of digital preservation, the scope of the standard, and the definitions of relevant terms, which go back to the terms of the OAIS reference model. The main part of the standard consists of the list of 34 requirements structured in 3 parts: organization, management of intellectual entities and their representations, and infrastructure and security.

Parameter	Information
Motivation for certification	The European repositories were part of DSA, and they want continue with the certification process, that means, keen on the overall audit process. On the case of US, there are other reasons to for seeking some kind of accreditation including the desire to demonstrate to management and reviewers that they were willing to undertake external, independent, international (ISO) evaluations in order to reach the highest standards in digital preservation. DNB - the main motivation for undergoing audit and certification was to have their own processes and documentation reviewed, scrutinized, and ideally approved by some external professionals. DANS – the main motivation was to discover the strengths and the weaknesses in the archiving activities of institute. This gave the confidence that they are well on their way to fulfil the requirements established.
Time to complete certification	ISO 16363 –Started at March 2011 and finished at Jan 2012 DIN 31644—Started at April 2011 and finished at December 2011
Final certification date	
Cost of preparing for certification	DSA - the initial submission "took approximately 4 days of staff time. A day was needed to work through the self-assessment form and record how they met each guideline (consulting with colleagues where necessary), and the rest of that time was spent updating existing documentation and making it available on-line..." DIN 31644 - Several staff members of the DNB were involved with varying intensity in the test audit. Total Person Months: 1,51 (1 PM = 17,6 PD) The effort that was expended, in the activities can be broken down into the following major areas: • preparation of evidence • assessing level of conformance to the standard • creation of new evidence if it does not already exist; • changing policy/procedures if the procedures do not meet the standard (pre-audit) • implementing policy/procedures
Cost of actual certificate	ISO 16363 —The costs of preparing for certification cover the time expended on all activities related to the work package, rather than just the preparations for the audit. According to the document, the costs were: • DANS 3 MM (500 working hours) • CINES 3 MM • UKDA 2 MM
Resources needed for certification (i.e. people, materials)	In the DIN 31644 and in the ISO 16363 it was used Excel spreadsheets; DSA provided a custom web form into which the repository could directly write their evidence and then reviewed by members of the DSA board.

Parameter	Information
Lessons learned	DSA—The European repositories had already acquired the DSA and, apart from DNB, were part of the DSA board. Extended Certification: ISO 16363 –The processes surrounding Extended Certification as defined in the Framework was not performed using ISO 16363 because this was a test situation and there was no willingness amongst the repositories that self-assessments should be made public unless this were a “live” situation. DIN 31644 —In general, the whole audit process needs to be well defined, documented and transparent. It must be clear to the auditors and to the audit candidate how the auditors are appointed and according to which methodology the auditors assess the audit candidate. Terms and deadlines of the audit process must be communicated. Formal Certification: ISO 16363 –This certificate was designed to undertaken at a reasonable cost and the Phase 2 visit to be for 2 days involving 2 auditors. For the test audits, they didn’t follow this plan, because it involved significant charges, paid by the repository being audited, and significant time (many months). However they believe, on the basis of these test audits, that the full process is will be practical once the audit methodology has been refined and published. DIN 31644—During the test process, DNB had some difficulties to separate clearly between the phases that would lead to Extended, respectively, Formal Certification. The auditors need tools and guidelines that help them conduct the Formal Certification, like in the phase that leads to Extended Certification. The tools and guidelines can to a large extent draw on what is defined for the self-audit, but there are additional questions to be considered.
Expected benefits of certification	DNB—with the certification, DNB will integrate the test audit results into its short and medium term digital preservation development strategy. Two concrete results were that the DNB will have to document more thoroughly its policy decisions and will have to reinforce its internal Quality Assurance. DANS–The test audit gave clear indications where they could improve the trustworthiness of our archive. With that, they can align the recommendations from the test audit as a primary guideline in the further development of their procedures and technical adaptations of their archive. CINES-DAD—The test audit gave some requirements for clarification and additional action plans that have also been worked out to address the few metrics which were not satisfied, and progress will be monitored regularly. SEDAC—the recommendations received from the test audit are important inputs into SEDAC's efforts to improve its capabilities and practices for data preservation and stewardship in collaboration with the Columbia University Libraries.
Return on Investment	The test audits have proved extremely valuable in testing all the standards and the processes. They have shown strengths and weaknesses in the processes of conformity assessment, including in the construction of an explicit audit methodology.

Parameter	Information
Overall evaluation of the certification effort	CINES-DAD—certainly helped them to evaluate the progress made since the previous audits and the relevance of the actions taken over the past couple of years, and was a good experience as a contribution to a standardization process. SEDAC—the certification provided an excellent opportunity to continue assessing its data management policies and procedures to identify opportunities for improvement. UKDA—the comments have proven instructive DNB—strengths as well as gaps were revealed, which is already a valuable result. Feedback from the auditors will influence the medium term development directions, especially in areas where the auditors suggested improvements. For the DNB, this knowledge gain is even more important than receiving a certificate to showcase. DANS—Have taken the recommendations from the test audit as a primary guideline in the further development of our procedures and technical adaptations of our archive. The test audit gave clear indications where they could improve the trustworthiness of their archive.

Parameter	Information
Source (Paper, Article, etc.)	Document written by Marie Waltz and other CRL staff in March 2011, that reports the audit and certification process to HathiTrust
Name of the organization	HathiTrust (www.HathiTrust.org)
Organization Profile	The HathiTrust digital repository was established by the University of Michigan Libraries in October 2008 and offers academic and research libraries the opportunity to combine resources to build and maintain a large scale repository. Participating members include research libraries in the United States and Europe. The majority of HathiTrust's content was digitized through the Google Books project, which has worked with libraries to scan books on library shelves. Additional content comes from the Internet Archive and from collections digitized by partner libraries. As of December 2010, HathiTrust had ingested approximately 7.5 million volumes.
Type of Certification (e.g. ISO, national, domain, institutional)	Trustworthy digital repository
Certification details	The audit process was based on the Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC) and other metrics developed by CRL through its various digital repository assessment activities. Thus, the certification process is subdivided in 3 categories of criteria specified in TRAC: • Organizational Infrastructure • Digital Object Management • Technologies, Technical Infrastructure, Security This certification applies specifically to the repository's ability to preserve and manage digital files of books digitized by the University of Michigan, Google, and the Internet Archive, as well as the digital files generated from books digitized by other providers that conform to comparable standards.
Motivation for certification	This assessment was undertaken to determine whether or not HathiTrust meets the commitments it has made in regard to the long-term preservation of digital scholarly content for the academic community and whether the repository complies with established criteria for trusted digital repositories.
Time to complete certification	Approximately one year (between November 2009 and December 2010)
Final certification date	December 2010
Cost of preparing for certification	The preparation for the audit included a process of collecting and updating documentation in order to make it easier to provide the documentation to other parties subsequently to the audit.
Cost of actual certificate	To continue a certification repository, HathiTrust has agreed to address the issues identified by Certification Advisory Panel and to make certain disclosures to CRL periodically.

Parameter	Information
Resources needed for certification (i.e. people, materials)	To this certification process, it was necessary: • Documentation gathered by CRL as well as data; • Documentation provided by HathiTrust; • Human resources from CRL and from HathiTrust • Certification Advisory Panel that includes leaders in collection development, preservation, library administration, and digital information technology
Lessons learned	On the basis of the audit, CRL identified areas in which HathiTrust will need to improve processes or provide greater disclosure of information about those processes. These areas correspond to specific TRAC criteria or to features of the repository that members of the Certification Advisory Panel believe are important to the CRL community. The specific areas identified for improvement are: • Definition of rights and ownership of HathiTrust enterprise assets • Succession or disposition plan for HathiTrust assets • clarify and strengthen the quality assurance and print archiving components of the HathiTrust program
Expected benefits of certification	With this certification, the HathiTrust expects to prove that provides services adequate to those interests and needs without material flaws or defects.
Return on Investment	According to the table provided by CRL that expresses the ratings, it reflects the existence of the existence of robust systems and sound processes in most areas, in particular in category C (Technologies, Technical Infrastructure, Security); and the still emerging systems and processes in category A (Organizational Infrastructure) and, to a lesser extent, in category B(Digital Object Management). In the course of the audit, the Certification Advisory Panel identified several issues that CRL urges HathiTrust to address to more fully satisfy the concerns of CRL libraries.
Overall evaluation of the certification effort	To maintain the HathiTrust's credibility, HathiTrust will need to undertake a regular cycle of audit and/or certification. To that end CRL expects that in addition to acting to remedy the issues identified above HathiTrust will also make certain disclosures on a regular basis. CRL and HathiTrust have agreed that on-going certification is contingent upon HathiTrust making disclosures every two years and will continue dialogue with CRL on the main priorities.

A2.2 Implementing standards and best practices

Parameter	Information
Source (Paper, Article, etc.)	The “livre blanc” version 3 intends to be educational and to be a subject of discussion and anticipation, especially on the impact and the modality of the implementation of the ISO 30 300 standards series. This document demonstrates reflections and collaboration between organizations, experts, and stakeholders of documentation management. Therefore, the main themes discussed are: • Central concept of ISO 30300 standard: Management System for records and all the representations of its concerns. • The interoperability of ISO 30 300 standard with the other management system standards, such as Quality (ISO 9000), Risks (ISO 31000), and Environment (ISO 14001)
Name of Standard	ISO 30300 ISO 9001 (Quality) ISO 14001 (Environment) ISO 27000 (Information security) ISO 31000 (Risks)
Developers of the standard	Countries members of the ISO/TC 46/SC11
Year of introduction of the standard	ISO standard 30300: 2011 ISO standard 9001: 2008 ISO standard 14004: 2004 ISO standard 27005: 2011 ISO standard 31000: 2009
Is there a certification for the standard?	According to the document, the authors said that the ISO 31000 is non-certifiable.

Parameter	Information
Small description of the standard	ISO 30300—In this standard, they consider that the creation and records management are integrant part of activities, processes and systems of any organism. This records lead to performance, responsibility, management risks and to the continuity of activities. Thus, this standard focuses on the implementation and operation of an effective Management System of Records (MSR) to managing records. A MSR allows an organization to define politics, objectives and guidelines to control records on the documentary systems and certifies that those systems answer to the organization exigencies and maintain that records as long as it required. ISO 9001—This ISO specifies the requirements relating to the Quality System Management when an organization must show its aptitude to provide regularly a product in conformity with the requirements of the customers and the legal and lawful requirements applicable, but also when it aims at increasing the satisfaction of its customers by the effective application of the system, including the processes for the continuous improvement of the system and the insurance of conformity to the requirements of the customers and the legal and lawful requirements applicable. ISO 14004—This certificate provides guidance on the establishment, implementation, maintenance and improvement of an environmental management system and its coordination with other management systems. ISO 27000—This ISO provides a model to establish, install, operationalize, keep and improve information protection in order to reach goals based on assessable risks and an acceptable risk level to organization to effectively define and manage their risks. ISO 31000—This norm provides principles and general guidelines for the implementation of risk management. This management should be traceable because records provide the foundation for improvement in methods and tools as well as the overall process.
Other references for the standard	

Parameter	Information
Source (Paper, Article, etc.)	Article written by Bruce Ambacher examines the RLG/NARA draft Audit Checklist for the Certification of Trusted Digital Repositories from the perspective of publicly funded repositories, especially government archives. Ambacher analyses the historical origins of the checklist; the comments received from government archives on the metrics in the draft document; the task force's adjudication of those comments and finally addresses some unresolved issues.
Name of Standard	Audit Checklist for the Certification of Trusted Digital Repositories
Developers of the standard	Research Libraries Group (RLG) US National Archives and Records Administration (NARA)
Year of introduction of the standard	The draft version was released for public comment in August 2005 with the comment period extending through mid-January 2006.
Is there a certification for the standard?	
Small description of the standard	This project focus on the premise that self-assessment is the essential first step in the development of a repository's certification program. The draft Audit Checklist was designed to be used and adapted by a variety of digital preservation programs including archives, museums, libraries, cultural heritage organizations, e-science programs, and data centers. Thus, the above-mentioned organizations can measure their established priorities and goals against the Checklist's metrics. According to the document, this draft is organized into four sections: • Organization covers governance, staffing, policies and procedures; • Financial sustainability; • Contracts; • Other obligations; Moreover, the three main frames of this draft are very explicit and understandable. For example, the program function addresses the whole range of repository preservation responsibilities including ingest (accessioning), archival storage, description, metadata, access, and preservation strategies. The Designated Community section focuses on both the records creators and users and the ability of the repository to meet their needs. The Technologies and technical infrastructure section concentrates on security, software and hardware, and similar issues that enable digital preservation.

Parameter	Information
Other references for the standard	While the draft Audit Checklist was undergoing public review and comment, it was also being tested by CRL in a variety of digital repositories, like Koninklijke Bibliotheek (KB), the Interuniversity Consortium for Political and Social Research (ICPSR), Portico, and LOCKSS. (http://www.crl.edu/content.asp?l1=13&l2=58&l3=142&l4=71) The version 1.0 also benefits from digital preservation work that is being done at the Digital Curation Centre (http://www.dcc.ac.uk/) and from the certification work of the Nestor project (Network of Expertise in Long-Term Storage of Digital Resources) in Germany (http://www.langzeitarchivierung.de/index.php?newlang=eng)

Parameter	Information
Source (Paper, Article, etc.)	Paper elaborated by Fran Berman, Robert H. McDonald, San Diego Supercomputer Center, Brian E. C. Schottlaender, Ardys Kozbial and UC San Diego Libraries. They want to describe a collaboration to develop and deploy Chronopolis, a model for preservation predicated on data grid infrastructure and replication.
Name of Standard	The Chronopolis model
Developers of the standard	The San Diego Supercomputer Center (SDSC), the UC San Diego Libraries (UCSDL), the National Center for Atmospheric Research (NCAR) and the University of Maryland (UMD).
Year of introduction of the standard	
Is there a certification for the standard?	According the document, Chronopolis is currently undertaking an audit of pilot participants in order to formalize the credibility and reliability of preservation providers.
Small description of the standard	This model describes a datagrid for replicated data preservation. The intent of the datagrid is to aggregate participants into a distributed, trusted repository that contains multiple copies of valued data collections and that provides varying degrees of access to those collections at each of the partner sites. In the model, each site can play any or all of several different roles for each collection, and can serve different roles for different collections.
Other references for the standard	Moore et. al, 2005 Model of Chronopolis Trust: adapted from Holland and Lockett, 2006

Parameter	Information
Source (Paper, Article, etc.)	Paper written by Norbert Fuhr, Giannis Tsakonas, Trond Aalberg, Maristella Agosti, Preben Hansen, Sarantos Kapidakis, Claus-Peter Klas, László Kovács, Monica Landoni, András Micsik, Christos Papatheodorou, Carol Peters and Ingeborg Sølvberg. This paper proposes a new framework for the evaluation of DLs, as well as for recording, describing and analyzing the related research field. This framework includes a methodology for the classification of current evaluation procedures. Completing, the objective is to provide a set of flexible and adaptable guidelines for DL evaluation.
Name of Standard	Doesn't have a particular name, but was called "Proposed guidelines – how to adopt the framework in the most productive way"
Developers of the standard	Norbert Fuhr, Giannis Tsakonas, Trond Aalberg, Maristella Agosti, Preben Hansen, Sarantos Kapidakis, Claus-Peter Klas, László Kovács, Monica Landoni, András Micsik, Christos Papatheodorou, Carol Peters and Ingeborg Sølvberg.
Year of introduction of the standard	
Is there a certification for the standard?	

Small description of the standard	The idea behind adopting this high level framework is to provide designers and evaluators with a better understanding of the role and the benefits of a well-designed and structured evaluation experiment. It is also a way to support evaluators in setting up effective experiments, so that their findings can be compared with similar or related studies and thus maximize their utility.
	The authors based their work on the framework for DL evaluation designed by Saracevic. He introduced a new framework based on four dimensions or components (construct, context, criteria and methodology) for describing evaluation activities. These dimensions can be used in a variety of ways, according to the level of development of the evaluation and the needs of its designers.
	Concluding, the framework developed, answers to the crucial questions:
	• Why evaluate—i.e. determine the aims of evaluation. In this stage strategic decisions are taken regarding the constructs, the relationships and the evaluation itself.
	• What to evaluate—this involves:
	  ○ Determining the constructs;
	  ○ Determining the type;
	  ○ Determining the target DL service;
	• How to evaluate—i.e. decide on the way to perform the evaluation:
	  ○ Planning the evaluation by selecting methods, criteria, metrics, samples (e.g. humans, collections)
	  ○ Executing the evaluation by selecting and analyzing data (main methods and alternatives)
	  ○ Presenting the results.

Other references for the standard	The work has been supported by the DELOS Network of Excellence on DLs, as part of the Information Society Technologies (IST) Program of the European Commission

Parameter	Information
Source (Paper, Article, etc)	Article written by Sangchul Song and Joseph JaJa develops a new methodology to address the long-term integrity of digital archives using rigorous cryptographic techniques. With this approach, a prototype system called ACE (Auditing Control Environment) has been built and tested in an operational large scale archiving environment.
Name of Standard	Approach about linked hashing technique
Developers of the standard	Sangchul Song and Joseph JaJa
Year of introduction of the standard	
Is there a certification for the standard?	
Small description of the standard	This methodology addresses the integrity of long-term archives using rigorous cryptographic techniques. This approach depends only on the use of hash functions and linking schemes, and is independent of an external infrastructure. On the other side, it's important to say, that the computational requirements of this approach are minimal and the overall solution can be implemented on any archive architecture. Completing this approach, they built a prototype system, called Auditing Control Environment (ACE) that executes this strategy. It means, that illustrate the auditing processes, and report on the performance on a large scale production environment.
Other references for the standard	More details about ACE and is methodology can be found on large collections in Chronopolis.

Parameter	Information
Source (Paper, Article, etc)	In this article, Robin L. and Emily B. Gore will give an overview of process models for preservation and the relationship of those process models to the development of standards related to trustworthy repositories.
Name of Standard	OAIS (Open Archival Information System) - as ISO 14721. InterPARES—International Research on Permanent Authentic Records in Electronic Systems Curation Lifecycle Model TDR - Trusted Digital Repositories METRICS Nestor project DRAMBORA—Digital Repository Audit Method Based on Risk Assessment TRAC—trusted repositories audit & Certification: Criteria & Checklist Audit and Certification of Trustworthy Digital Repositories - designated CCSDS 652.0-R1 Requirements for Bodies Providing Audit and Certification of Candidate Trustworthy Digital Repositories – designated CCSDS 000.0-R-0
Developers of the standard	OAIS was developed by Consultative Committee for Space Data Systems (CCSDS) Curation Lifecycle Model - DCC (Digital Curation Centre) TDR - RLG and OCLC METRICS DRAMBORA—Digital Curation Centre (DCC) and Digital Preservation Europe (DPE) TRAC—CRL Certification of Digital Archives Project and the RLG-NARA task force CCSDS 652.0-R1—MOIMS-RAC CCSDS 000.0-R-0—MOIMS-RAC
Year of introduction of the standard	OAIS – in 2003 was formalized and published InterPARES—Started to develop in 1999 and the last phase, date 2012; TDR—March 2000 METRICS Nestor project –December 2004 TRAC—February 2007 CCSDS 652.0-R1—October 2009
Is there a certification for the standard?	On the TDR case, there is an organization that certificate, called CRL, Center for Research Libraries

Parameter	Information
Small description of the standard	OAIS—as a process model, gives a framework for further, more granular standards development and establishes an ontology for communication among repositories. InterPARES—focuses on a model for ensuring the preservation, accuracy, reliability, and authenticity of electronic records. Curation Lifecycle Model - The model aims to illustrate the steps or high-level processes necessary for long-term preservation, and is designed to be used in conjunction with relevant standards to plan curation and preservation activities to different levels of granularity TDR—as one whose mission is to provide reliable, long-term access to managed digital resources for its designated community, now and in the future. METRICS Nestor—define a first catalogue of criteria for trustworthiness and to prepare for the certification of digital repositories in accordance with nationally and internationally coordinated procedures DRAMBORA—is a methodology for self-assessment, encouraging organizations to establish a comprehensive self-awareness of their objectives, activities, and assets before identifying, assessing, and managing the risks implicit within their organization. TRAC—Is broken into 3 sections. The main goal is provide tools for the audit, assessment, and potential certification of digital repositories; establishes the documentation requirements for audit; delineates a process for certification; and establishes appropriate methodologies for determining the soundness and sustainability of digital repositories. CCSDS 652.0-R1—is a draft standard that articulates the audit and certification criteria for trustworthy digital repositories. It is in the balloting and revision process and expected to be released very soon as the new international standard for certification. CCSDS 000.0-R-0—will incorporate new requirements and guidance for agencies to be accredited as complying with ISO/IEC 17021 with the objective of auditing and certifying candidate Trusted Digital Repositories (TDR).
Other references for the standard	For OAIS, the related standards development emerged including Producer-Archive Interface Methodology Abstract Standard(PAIS) and the PREMIS Data Dictionary for Preservation Metadata.

Parameter	Information
Source (Paper, Article, etc)	Draft for public comment published by nestor Working Group Trusted Repositories – Certification
Name of Standard	Catalogue of Criteria for Trusted Digital Repositories
Developers of the standard	Dobratz, Susanne, Dr. Hänger, Andrea, Huth, Karsten, Kaiser, Max, Dr. Keitel, Christian, Dr. Klump, Jens, Rödig, Peter, Dr. Rohde-Enslin, Stefan, Dr. Schoger, Astrid, Schröder, Kathrin, Strathmann, Stefan, Wiesenmüller, Heidrun
Year of introduction of the standard	This version was published in June 2006, Frankfurt am Main
Is there a certification for the standard?	In this project, there isn't an organization that verifies the implementation of standards. But it's explicit in the document that: "The procedure of evaluation and certification is to be continued in the follow-on project "nestor II" which will include national and international standardisation activities."
Small description of the standard	The criteria catalogue is principally aimed at memory organisations (archives, libraries, museums) and serves as a manual for devising, planning and implementing a trusted digital long-term repository. It can also be used at all stages of development for self-checking. In addition, this catalogue is intended to provide guidance to all institutions currently administering archives, commercial and non-commercial service providers, and third party service providers. The criteria are each accompanied by extensive explanations and concrete examples from different fields.
Other references for the standard	The OAIS reference model together with its functional entities and information model serves as the basis for providing common terms and for structuring the criteria catalogue.

Parameter	Information
Source (Paper, Article, etc)	It is a special article that includes 3 feature articles about the certification of digital repositories. Article 1—written by Seamus Ross and Andrew McHugh present an introduction to audit and certification of digital repositories, as well as some relevant initiatives in which the Digital Curation Centre (DCC) of the UK will engage. Article 2—In this article, Robin Dale discusses the development of certification methodology through the work of the RLG-NARA Digital Repository Certification Task Force, the Audit Checklist for Certifying Digital Repositories, and the Center for Research Libraries Audit and Certification of Digital Archives project. Article 3 —The last section, is related by Susanne Dobratz and Astrid Schoger and provide an overview of two certification-related initiatives in Germany: the Deutsche Initiative für Netzwerkinformation (DINI) Certificate for Document and Publication Repositories and the Working Group on Trusted Repository Certification of the Network of Expertise in Long-term STOrage of Digital Resources (nestor)
Name of Standard	Article 2: • The RLG-NARA Audit Checklist • The CRL Audit and Certification of Digital Archives Project Article 3: • DINI • NESTOR
Developers of the standard	Article 2: • the RLG-NARA Digital Repository • Certification Task Force • Center for Research Libraries (CRL) Article 3: • The German Initiative for Networked Information (DINI) • nestor Working Group on Trusted Repository Certification
Year of introduction of the standard	

Parameter	Information
Is there a certification for the standard?	Article 1: The authors hope that in UK the Digital Curation Center working with national, European, and international bodies, can achieve a mandate to manage audit processes and to oversee the awarding of certified status. The DCC will support its implementation of audit and certification services through training events, targeted at information holders and service providers and aimed at offering insights into a range of activities and documentation needed to prepare for audit. Article 2: The authors considered that Audit and certification are tools that have been under development through the RLG-National Archives and Records Administration (NARA) Digital Repository Certification Task Force. In the case of The CRL Audit and Certification of Digital Archives Project, the colleagues that are working in the same project, like nestor Working Group on Trusted Repository Certification and the Digital Curation Centre (DCC) in the UK have expressed an interest – and are stakeholders – in shaping and managing any certification process that will affect repositories within their respective countries. Article 3: For the DINI, only the DINI office or an authorized working group is responsible for awarding the DINI Certificate

Parameter	Information
Small description of the standard	Article 1: In this article, they consider that the self-audit is the obvious "entry-level" class and it could be a useful internal process. Products like the RLG-NARA draft audit checklist can be used or extended to facilitate it. The use of this self-audits could reduce the costs that an external audits need. By other side, the external audits are likely to cover every aspect of a repository's business, including systems, finances, personnel, and procedures. It is unlikely that every repository will need to acquire formal certification if they are to achieve trusted status. Article 2: The RLG-NARA Audit Checklist According the authors, the task force developed a comprehensive list of criteria that could be used to audit large scale repositories that assumed a variety of data curation responsibilities. For this, five different frameworks were utilized to conceptualize the nature of the required criteria or audit metrics. Each presented a different perspective, allowing the task force to identify and fill gaps. The resulting framework reflects four overarching categories of criteria: • Organizational infrastructure; • Repository functions, processes, and procedures; • Designated community and the intended uses of information; • Technology and technical infrastructure. The CRL Audit and Certification of Digital Archives Project This project intends to refine, test and deliver specifications for the auditing processes, develop a plan for certification, and will outline a business model for the certifying agency or entity best suited to carry out those processes on a continuing basis. It involves three work phases: Designing the audit process and refining the audit criteria and terminology to be used. Model the audit process through test audits of three digital archives Specify the economic and service models appropriate to undertake those processes on a continuing basis. Article 3: DINI This certificate distinguishes the repository from common institutional web servers and assures potential users and authors of digital documents that a certain level of quality in repository operation is warranted. In addition, DINI sees its certificate as an instrument to support the Open Access concept. It can be viewed as a "soft certificate," where the coaching idea prevails, and works on the basis of self-disclosure by the repositories. NESTOR The goal of nestor is to create a network of expertise in the long-term storage of digital resources for Germany, comparable to initiatives like the Digital Preservation Coalition in the UK. This certificate aims to document the trust worthiness of digital repositories, data producers, and service providers not only in higher education institutions but also in national and state libraries and archives, museums, and data centers. Trustworthiness is important to potential customers, who are the producers of digital information on the one hand and the readers of the deposited information on the other hand.

Parameter	Information
Other references for the standard	Article 2: RLG-NARA Task Force on Digital Repository Certification. Audit Checklist for the Certification of Digital Repositories: Draft for Public Comment, August 2005.

Parameter	Information
Source (Paper, Article, etc)	Article that explains the building of a Framework for Applying OAIS to Distributed Digital Preservation by Katherine Skinner, Eld Zierau, Matt Schultz
Name of Standard	Building of a Framework for Applying OAIS to Distributed Digital Preservation
Developers of the standard	The Educopia Institute, the Royal Library of Denmark, the Library of Congress, Chronopolis, DuraSpace Foundation, MetaArchive Cooperative, LOCKSS, Data-PASS, California Digital Library, Archivematica, and Internet Archive
Year of introduction of the standard	
Is there a certification for the standard?	
Small description of the standard	According to the article, a lot of organizations (previously mentioned) are developing a framework to identify, define and provide a documented model for the range of relationships and interactions that occur in Distributed Digital Preservation environments. The group defines DDP as "the use of replication, independence, and coordination to address the known threats to digital content to ensure its accessibility through time". The main goal of these organizations is to effectively document the practice of distributed digital preservation through a serial of rules. This development will be based on interviews and feedback from all groups of distributed digital preservation.
Other references for the standard	
Source (Paper, Article, etc)	Article written by MacKenzie Smith, from MIT Libraries and Reagan W. Moore, from San Diego Supercomputer Center.
Name of Standard	PLEDGE Project RLG/NARA Trusted Digital Repository Checklist PREMIS metadata schema
Developers of the standard	PLEDGE - US National Archives and Records Administration; MIT Libraries; University of California San Diego Libraries RLG/NARA – Research Library Group (RLG) and the US National Archives and Records Administration(NARA)
Year of introduction of the standard	RLG/NARA – 2005
Is there a certification for the standard?	

Parameter	Information
Small description of the standard	PLEDGE—This project consists in investigate the diversity of policies in use by two operational digital archives: the DSpace repository for digital information life cycle management and the integrated Rule-Oriented Data System (iRODS) for storage virtualization and digital object persistence. The team are identifying and categorizing these policies, and defining associated rules and state information to make them machine encodable and wherever possible, enforceable. They try to mapped the PLEDGE polices to the recently published RLG/NARA Audit Check list for the Certification of Trusted Digital Repositories(TDR) and evaluate what is missing from the TDR checklist where those policies translate into multiple operational rules. In effect, they try to demonstrate the set of rules that automatically validate the trust worthiness of a repository. RLG/NARA—The intention of this audit checklist is providing digital archivists with criteria for assessing the “trustworthiness” of a particular digital repository or archive (often referred to as a trusted digital repository or TDR). PREMIS—This schema serves to demonstrate how a preservation environment might be assessed to insure that the system is complete. That means no required process are overlooked and no required preservation metadata attributes are missing.
Other references for the standard	

Parameter	Information
Source (Paper, Article, etc)	Presentation that explains the TRAC criteria and adaptation of certification to User Requirements
Name of Standard	TRAC
Developers of the standard	CRL and RLG/NARA Task Force on Digital Repository Certification
Year of introduction of the standard	
Is there a certification for the standard?	
Small description of the standard	TRAC is a principal tool used by CRL in its auditing and certification of digital repositories. The same criteria can be applied to many types of repositories. Normally, the TRAC users are: • Digital repositories; • Publishers; • Librarians; • Researchers and the general public. The value of this methodology is associated to its flexibility, it means, the rigor of an audit can vary, and of course, the required documentation associated will change. If a user group may require greater oversight of a repository, TRAC need to adapt to that change. Resuming, TRAC can help in many ways like assist in identifying needs and costs of archiving data, help in repository planning, assist in communication between interest group (giving users a framework for communicating), define an organizational framework for a repository of any size, etc. According to CRL, the average cost for an audit was $65,000, but it is possible that varies depending on the level of importance placed on the audit.
Other references for the standard	Repositories audited: • ICPSR (Inter-university Consortium for Political and Social Research) • Portico • Koninklijke Bibliotheek (KB) – Elsevier journals repository

Parameter	Information
Source (Paper, Article, etc)	Document that shares information regarding Data Seal of Approval, by Laurents Sesink, René van Horik and Henk Harmsen
Name of Standard	Data Seal of Approval (DSA)
Developers of the standard	Laurents Sesink, René van Horik and Henk Harmsen
Year of introduction of the standard	2010
Is there a certification for the standard?	The criteria for assigning the Data Seal of Approval to data repositories are in accordance with, and fit in with, national and international guidelines for digital data archiving such as Kriterienkatalog vertrauenswürdige digitale Langzeitarchive as developed by NESTOR; Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) published by the Digital Curation Centre (DCC) and DigitalPreservationEurope (DPE); and Trustworthy Repositories Audit & Certification (TRAC): Criteria and Checklist of the Research Library. Furthermore the following has been taken into account: Foundations of Modern Language Resource Archives of the Max Planck Institute and Stewardship of Digital Research Data: A Framework of Principles and Guidelines published by the Research Information Network.
Small description of the standard	The quality Guidelines formulated in the Data Seal of Approval are of interest to data consumers and institutions that create digital data, to organizations that archive data, and to consumers of data. The objectives of the Data Seal of Approval are to safeguard data, to ensure high quality and to guide reliable management of data for the future without requiring the implementation of new standards, regulations or high costs.
Other references for the standard	http://www.datasealofapproval.org/media/filer_public/2013/09/27/dsa-booklet_1_june2010.pdf; https://assessment.datasealofapproval.org/assessment_55/seal/html/; https://assessment.datasealofapproval.org/assessment_47/seal/html/; http://www.dcc.ac.uk/resources/case-studies/ads-dsa

Parameter	Information
Source (Paper, Article, etc)	Document that shares information regarding ISO 16363, by Michael Witt and Matthew Kroll - Purdue University, David Minor - University of California - San Diego, Bernie Reilly - Center for Research Libraries.
Name of Standard	ISO 16363 - Trustworthy Digital Repository Certification in Practice
Developers of the standard	Michael Witt and Matthew Kroll - Purdue University, David Minor - University of California - San Diego, Bernie Reilly - Center for Research Libraries.
Year of introduction of the standard	2012
Is there a certification for the standard?	The criteria for assigning ISO 16363 certification process from a repository that was under an audit (Purdue University), a repository that has recently been certified as a trustworthy digital repository (Chronopolis Digital Preservation Network, University of California, San Diego), and an auditor (Center for Research Libraries). After a concise overview of the certification process, each panellist offered insight and practical tips based on their experience and participate in a moderated discussion that includes questions and comments from the audience.
Small description of the standard	In 2003, the Research Libraries Group and National Archives and Records Administration (NARA) convened a task force to address the issue of digital repository certification. Further collaboration with the Center for Research Libraries (CRL), nestor, the Digital Curation Center, and others led to development of Trustworthy Repositories Audit & Certification: Criteria and Checklist, otherwise known as the TRAC Checklist, which was published in 2007 . Other, important work taking place around this same time in Europe included, but was not limited to, the development of the Catalogue of Criteria for Trusted Digital Repositories by nestor, DRAMBORA (Digital Repository Audit Method Based On Risk Assessment) from the DCC and DigitalPreservationEurope, and the Data Seal of Approval by the Dutch Data Archiving and Networked Services. The TRAC Checklist has since been updated by a group of collaborators, leading up to the creation of a birds-of-a-feather group led by David Giaretta that became the MOIMS-RAC (Mission Operations Information Management Services Repository Audit and Certification) Working Group of the Consultative Committee for Space Data Systems. The working group and collaborators worked with the International Organization of Standardization (ISO) to formalize TRAC as ISO 16363:2012 Audit and Certification of Trustworthy Digital Repositories. On February 14, 2012, this work reached stage 60:60, “International Standard published”. Requirements for auditors are currently going through a similar standardization process for its complement, ISO/DIS 16919: Requirements for Bodies Providing Audit and Certification. ISO 16363 uses language and concepts from the Open Archival Information Systems (OAIS) reference model, and it enables the assessment and certification of a repository as being a trustworthy digital repository (TDR).

Other references for the standard	Waters, Donald & Garrett, John. 1996. Preserving Digital Information. Report of the Task Force on Archiving of Digital Information. Retrieved on March 4, 2012, from http://www.clir.org/pubs/reports/pub63watersgarrett.pdf. Online Computer Library Center & Center for Research Libraries. 2007. Trustworthy Repositories Audit & Certification: Criteria and Checklist. Retrieved on March 4, 2012, from http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf. Digital Repository Audit and Certification Wiki. Retrieved on March 4, 2012, from http://wiki.digitalrepositoryauditandcertification.org/bin/view. Overview of the Mission Operations and Information Management Services Digital Repository Audit and Certification Working Group (MOIMS-RAC). Retrieved on March 4, 2012, from http://cwe.ccsds.org/moims/default.aspx. ISO 16363:2012 Audit and Certification of Trustworthy Digital Repositories. 2012. International Organization for Standardization. Retrieved on March 4, 2012, from http://public.ccsds.org/publications/archive/652x0m1.pdf. International Organization for Standardization: ISO 16363:2012. Retrieved on March 4, 2012, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56510. ISO/DIS 16919: Requirements for Bodies Providing Audit and Certification. 2012. International Organization for Standardization. Retrieved on March 4, 2012, from http://public.ccsds.org/publications/archive/652x1m1.pdf.

A2.3 Practical experience from memory institutions

Parameter	Information
Source (Paper, Article, etc)	Report on the analysis, evaluation and risk areas of the IT field in the National Library of Estonia
Name of the organization	National Library of Estonia
Organization Profile	The National Library of Estonia collects, stores and makes documents published in Estonia or about Estonia publicly accessible, registers Estonian national bibliography and prints output statistics and assigns international standard numbers. There is also a digital archive named DIGAR that collects and preserves Estonian publications.
Type of Certification (e.g. ISO, national, domain, institutional)	National information security standard (ISKE)
Certification details	ISKE is an information security standard that is developed for the Estonian public sector. It is compulsory for state and local government organisations who handle databases/registers A three-level baseline system means three different sets of security measures for three different security requirements have been developed (different databases and information systems may have different security levels).
Time to complete certification	1 month
Final certification date	October 8, 2009
Cost of actual certificate	1606 €
Resources needed for certification (i.e. people, materials)	Interviews with 4 specialists, information technology infrastructure scheme, ordinance of NLE's activities, results from previous inventory, materials on system development
Lessons learned	

Parameter	Information
Source (Paper, Article, etc)	Response to a questionnaire conducted by the National Library of Estonia in 2011
Name of the organization	The National Archives of Estonia
Organization Profile	The National Archives of Estonia is the centre of archival administration in Estonia. The main task of the National Archives is to ensure preservation and usability of society's written memory, documented cultural heritage for today's and future generations
Type of Certification (e.g. ISO, national, domain, institutional)	Information security (ISKE)
Certification details	ISKE is an information security standard that is developed for the Estonian public sector. It is compulsory for state and local government organisations who handle databases/registers A three-level baseline system means three different sets of security measures for three different security requirements have been developed (different databases and information systems may have different security levels).
Time to complete certification	
Cost of actual certificate	
Resources needed for certification (i.e. people, materials)	Interviews with specialists
Lessons learned	
Overall evaluation of the certification effort	The audit went well and the National Archives of Estonia found the proposed recommendations, conclusions and suggestions valuable for the further development of its digital archive.