The International Journal of Digital Curation
Issue 1, Volume 5 | 2010

The Use of Quality Management Standards in Trustworthy Digital Archives

Susanne Dobratz,
Humboldt-Universität zu Berlin,
University Library
Peter Rödig and Uwe M. Borghoff,
Universität der Bundeswehr München,
University of the Federal Armed Forces Munich
Björn Rätzke,
Rätzke IT-Service
Astrid Schoger,
Bayerische Staatsbibliothek,
Bavarian State Library

Abstract

Quality management is an essential part in creating a trustworthy digital archive. The German network of expertise in Digital long-term preservation (*nestor*), in cooperation with the German Institute for Standards (DIN), has undertaken a small study to analyse systematically the relevance and usage of quality management standards for long-term preservation and to filter out the specific standardisation need for digital archives. This paper summarises the results of the study. It gives an overview on the differences in understanding the task "quality management" within different organisations and how they carry out appropriate measures, such as documentation, transparency, adequacy, and measureability in order to demonstrate the trustworthiness of their digital archive.[1]

[1] This article is based on the paper given by the authors at iPRES 2008; received February 2010, published June 2010.
The *International Journal of Digital Curation* is an international journal committed to scholarly excellence and dedicated to the advancement of digital curation across a wide range of sectors. ISSN: 1746-8256 The IJDC is published by UKOLN at the University of Bath and is a publication of the Digital Curation Centre.

Introduction

In 1996, the Task Force on Archiving of Digital Information by The Commission on Preservation and Access and the Research Libraries Group called for a certification programme for long-term preservation repositories: "… repositories claiming to serve an archival function must be able to prove that they are who they say they are by meeting or exceeding the standards and criteria of an independently-administered program for archival certification..." (Task Force on Archiving Digital Information, 1996). Some investigations in creating criteria and measuring the risk for a long-term preservation of digital objects have been carried out by several stakeholders, such as the Cornell Library Virtual Remote Control Tool Project of Cornell University (McGovern, Kenney, Entlich, Kehoe & Buckley, 2004), the ERPANET project[2], and - most recently - by the Digital Repository Certification Task Force of the Research Libraries Group (RLG) and OCLC, the Digital Curation Centre (DCC) in cooperation with the European Commission-funded project Digital Preservation Europe (DPE), and the German *nestor* project.

The existence of such criteria has led to an increased in the development and installation of digital archives over recent years. It also created new discussions on the importance and applicability of existing standards as many of the organisational criteria in those catalogues refer to specific ISO quality management standards, such as ISO 9000 (2000) and so on.

During the creation of a DIN/ISO Working Group in Germany for defining the criteria for trustworthy digital archives, the essential question on the recent degree of acceptance and usage of quality management standards within the cultural heritage sector (libraries, archives, museums) arose. As a consequence, the German Institute for Standards (DIN) sponsored a small study to analyse systematically the relevance and usage of quality management standards for long-term preservation, and to filter out the specific standardisation need for digital archives. This study has two parts: (1) a survey undertaken at a number of different digital archives; and (2) an analysis of standards for the management of quality, processes, and security. It discusses the relevance and applicability in practice of those standards for use within a digital preservation environment. It shows how and which standards related to quality management are in use in digital archives of different kinds in Germany: libraries, archives, data centres, publishers, museums.

Long-term Preservation and Trustworthy Digital Archives

One of the central challenges to long-term preservation in a digital repository is the ability to guarantee the authenticity and interpretability (understandability) of digital objects for users across time. This is at risk due to the aging of storage media, the obsolescence of underlying systems and application software, as well as changes in technical and organisational infrastructures. Malicious or erroneous human actions also put digital objects at risk. Trustworthy long-term preservation in digital repositories requires technical, as well as organisational, resources. A trustworthy digital repository for long-term preservation has to operate according to the repository's aims and specifications. Key concepts that demonstrate trustworthiness are, for example,

[2] Erpanet Project (2003): Risk Communication Tool: http://www.erpanet.org/guidance/docs/ERPANETRiskTool.pdf

transparency and documentation. In order to evaluate trustworthiness, the measures taken in order to minimize the risk potential for the digital objects representing the important values in digital archives, have to be appropriate, measureable, and traceable.

Trustworthiness.

Trustworthiness of a system means that it operates according to its objectives and specifications (it does exactly what it claims to do). From an information technology (IT) security perspective, integrity, authenticity, confidentiality, non-repudiation, and availability are important building blocks for trustworthy digital archives. Integrity refers to the completeness and exclusion of unintended modifications to archive objects. Unintended modifications could arise, due to malicious or erroneous human behavior, or from technical imperfection, damage, or loss of technical infrastructure. Authenticity here means that the object actually contains what it claims to contain. This is provided by documentation of the provenance and of all changes to the object. Availability is a guarantee (1) of access to the archive by potential users and (2) that the objects within the archive are interpretable. The availability of objects is a key objective, which must be fulfilled in relation to the designated community and its requirements. Confidentiality means that information objects can only be accessed by permitted users.

Potential interest groups for trustworthiness are:

- archive users who want to access reliable information – today and in the future,
- data producers and content providers for whom trustworthiness provides a means of quality assurance when choosing potential service providers,
- resource allocators, funding agencies and other institutions that need to make funding and granting decisions, and
- long-term digital archives that want to gain trustworthiness and demonstrate this to the public - either to fulfil legal requirements or to survive in the market.

There is a wide range of preservation archives that exist or are under development: from national and state libraries and archives with deposit laws; to media centres having to preserve e-learning applications; to archives for smaller institutions; to world data centres in charge of “raw” data. Trustworthiness can be assessed and demonstrated on the basis of a criteria catalogue.

Documentation.

The goals, concepts, specifications, and implementation of a long-term digital archive should be documented adequately. The documentation demonstrates the development status internally and externally. Early evaluation based on documentation may also prevent mistakes and inappropriate implementations. Adequate documentation can help to prove the completeness of the design and architecture of the long-term digital archive at all steps. In addition, quality and security standards require adequate documentation.

Transparency.

Transparency is achieved by publishing appropriate parts of the documentation, which allow users and partners to gauge the degree of trustworthiness for themselves. Producers and suppliers are given the opportunity to assess to whom they wish to entrust their digital objects. Internal transparency ensures that any measures can be traced, and it provides documentation of digital archive quality to operators, funders, management, and employees. Those parts of the documentation not suitable for the general public (e.g., company secrets, security-related information) can be restricted to a specified group or body (e.g., certification agency). Transparency establishes trust, because it allows interested parties direct assessment of the quality of the long-term digital archive.

Adequacy.

According to the principle of adequacy, absolute standards cannot be given. Instead, evaluation is based on the objectives and tasks of the long-term digital archive in question. The criteria have to be seen within the context of the special archiving tasks of the long-term digital archive. Some criteria may therefore prove irrelevant in certain cases. Depending on the objectives and tasks of the long-term digital archive, the required degree of fulfilment for a particular criterion may also differ.

Measurability.

In some cases - especially regarding long-term aspects - there are no objectively assessable (measurable) features. In such cases we must rely on indicators showing the degree of trustworthiness. As the fulfilment of a certain criteria always depends on the designated community, it is not possible to create “hard” criteria for some of them, for example, how can it be measured, what adequate metadata is? Transparency also makes the indicators accessible for evaluation.

Quality Management (QM) and Standards

Quality of products, processes, and systems is a key factor for economic success in an open world. Implementing and operating a quality management system is vital for many organisations in order to survive in the market. However, public administration bodies are also interested in a more efficient and effective use of funding for public services. Therefore, a number of principles, methods, practices, and techniques have been developed over the past few decades. Many of them are consolidated, broadly accepted and published as standards.

In order to get an initial idea of core concepts, we refer to the well known standard ISO 9000 (2000). Quality management is defined as coordinated activities to direct and control an organisation with regard to quality. The activities generally include the establishment of a quality policy and quality objectives, quality planning, quality control, quality assurance, and quality improvement. These specific activities are the task of a quality management system. Of course, ISO 9000 (2000) also provides a definition of the term quality. It is defined as the degree to which a set of inherent characteristics fulfils requirements. And a requirement is a need or expectation that is stated, generally implied, or obligatory.

Background and Focus of This Study

Since 2006, the German Ministry of Economics and Technology (BMWi) has been financing a long-term project called Innovation with Norms and Standards (INS). The primary aim is to provide optimal business conditions for future innovation and to support their ability to act in the global market. In 2008, within the INS initiative, DIN and *nestor* carried out a project targeting the standardisation of topics relevant to long-term preservation especially (1) quality management for trustworthy digital archives, as documented in this study, and (2) standardisation of ingest processes. This project continues the work begun in 2007 where the needs for standardisation in digitisation and long-term preservation were collected and investigated in two separate studies.

The ideas discussed in this paper are based on early developments for a framework describing the requirements and functionalities for archiving systems that focus on the long-term preservation of digital materials, the Open Archival Information System (OAIS) (2003). From that work the Digital Repository Certification Task Force of the Research Libraries Group (RLG) and OCLC derived attributes and responsibilities for so-called trusted digital repositories (2002) and in February 2007 finally released, under the title Trustworthy Repositories Audit and Certification Checklist (TRAC) (2007), a checklist for conducting audits, worked out by the Auditing and Certification of Digital Archives project run by the Center for Research Libraries (CRL). The German *nestor* project developed a catalogue of criteria in 2004 and a second version in 2008. *nestor* is concentrating on the specific national situation and is developing the catalogue as a guideline for the concept and design of a trustworthy digital archive (*nestor* Working Group on Trusted Repositories Certification, 2006). The Digital Curation Centre (DCC) in cooperation with the European Commission-funded project Digital Preservation Europe (DPE) conducted some test audits based on the first draft of the RLG-NARA/CRL checklist (OCLC, 2007) and developed a risk-management tool for trusted digital long-term repositories, called Digital Repository Audit Method Based on Risk Assessment (DRAMBORA, 2007). Within the PLANETS project[3], the development of a Preservation Test Bed to provide a consistent and coherent evidence base for the objective evaluation of different preservation protocols, tools and services and for the validation of the effectiveness of preservation plans takes place. In January 2007 the OCLC/RLG-NARA Task Force, CRL, DCC, DPE and *nestor* archives (2007) agreed upon a set of common principles, ten basic features of digital preservation. The current TRAC checklist is the basis for an ISO standardisation effort led by David Giaretta (DCC) and carried out under the umbrella of the OAIS standards family of the Consultative Committee for Space Data Systems (CCSDS) via ISO TC20/SC13.

The questions that all those standardisation efforts have to answer are:

- Is a new single standard for trustworthy digital archives needed?
- How does this standard link to existing standards?
- Is an evaluation or even a certification of trustworthy digital archives desireable and useful?

[3] Planets – Preservation and Long-term Access Through Networked Services: http://www.planets-project.eu/

The current study analyses several quality management standards regarding their applicability for the evaluation of trustworthiness of digital archives. It exacts to what extent the standardisation of criteria for trustworthy digital archives can be based on existing standards and identifies domain-specific standardisation needs.

Identifying and practising quality measures within a long-term preservation context attracts a great deal of attention both nationally and internationally.

While the amount of digital data explodes and a growing number of institutions are establishing digital archives, there is still a deficit in standards and commonly accepted measures used for the development and the quality control during the creation of such archives. Internationally there are two options: firstly to define catalogues of criteria; and secondly to work out risk potentials based on the specific goals of the archives in question. This way, the links to existing standards and norms are used without defining and specifying the relation to or the use of those standards within a long-term preservation archive. Furthermore, it is useful to distinguish between the efforts required for standardisation and that for certification. The latter issue can only be carried out if reliable standards, criteria, and most importantly, appropriate measurements exist. Due to the varying goals and realisations of digital archives it is necessary to identify categories of digital archives that may use the same or similar standards.

The main focus of this study is to assess the applicability of existing standards in the long-term preservation field. Certification methods and schemas will be the subject of a follow-up study in 2010.

Methodology

Identification of Relevant Quality Management Standards

The first step was to identify and characterise the QM standards that are potentially useful for planning and operating trustworthy digital archives. Attributes already defined for determining the trustworthiness of digital archives serve as a guideline for selecting the initial set of relevant standards. This first selection provides a basis for designing the questions in the questionnaire in order to find out more easily which standards exist, are under discussion or have already been applied or rejected. Moreover, this set of standards serves as a basis for a deeper analysis of the applicability of QM standards in long-term preservation based on the results of the questionnaire.

Survey of Quality Management Standards Used in Long-term Preservation

Next, the questionnaire and survey were designed. We asked all institutions involved in the 2004 survey on attributes and technologies used for setting up digital archives to be involved. This survey, conducted by the *nestor* Working Group on Trusted Repository Certification (nestor WG TDR), finally resulted in the design of the first *nestor* catalogue released in June 2006. (*nestor* Working Group on Trusted Repositories Certification, 2006)

In addition, institutions that were known to be working on establishing a digital archive, as well as commercial partners (e-newspapers, repository services providers), were included in the study. 53 institutions representing the digital archive landscape in Germany were approached: libraries, libraries at universities, museums, archives (public bodies), archives (private, corporate bodies), and commercial vendors.

The design of the questionnaire needed to mirror some of the criteria in the *nestor* catalogue as well as make visible those activities that could be interpreted as quality management, even though might not be recognised as such by the institution. We asked for the institution's organisational and professional profile as well as for their policy on their digital long-term preservation archive and the type and number of digital objects held. Several specific questions focused on the use of standards and quality management.

The 44 questions were as follows[4]:

A	**Organisation**
1-6	Contact data of responsible manager
	Information about the organisation itself
7	Status of the organisation (public, private)
8	Type of organisation (administration, university, library, archive, museum, …)
9	Research area (astronomy, biology, chemistry, …)[5]
10	Mission of the the institution
11	Age, growth, budget of institution
	Information about the digital archive
12	Policies
13	Growth of digital objects
14	Financial concept
15	How can the existence of the digital collection granted after structural changes in organisation?
16	Quality management (yes, no)
17	Quality management: what is done precisely?
18	Do you have a quality manager?
19	Have you concerns about standards and norms?
20	Have you discussed standards and norms?
21	Has the applicability of standards been analysed in your intitution?
22	Would you need support and training in order to introduce standards?
23	Do you follow standards with a quality or security issue? (followed by a detailed list of selected standards from the theoretical analyses and by checkboxes indicating the degree of use and certification)
24	Do you follow other standards?
25	Are you developing software?
26	Do you use a service provider for the operation of the digital archive? (relation to provider)
27	Does your service provider perform a quality management?
B	**Object Management**
30	Do you have formal regulations with producers?

[4] Details and the whole questionnaire are given in the final study report to be published by *nestor*.

[5] It was a disadvantage that no formal subject schema was used here, we oriented on a subject schema of CRL collegues.

31	Do you have a concept for keeping the quality in relation to the producers?
32	Do you carry out quality control measures for objects and metadata?
28	Types of objects (carrier, format, content)
29	Selection criteria (yes, no, planned, published)
33	Do you know your user community?
34	Have you collected the user community needs?
35	Do you provide specific interfaces for your users?
36	Do you monitor user satisfaction?
37	Do you have a concept for keeping the quality in relation to your users?
C	**Infrastructure and Security**
38	Have you defined the processes and organisational structures for the operation of your archive?
39	Have you documented the processes and organisational structures for the operation of your archive?
40	Do you have an IT-concept for your institution?
41	Do you have a security concept for your institution?
42	Have you documented or contracted the committment to upgrade your hard- and software?
	Trustworthy digital archive
43	Would the development of a special standard for trustworthy digital archives be helpful for your development of a long-term preservation archive?
44	Would you be interested in a certification as trustworthy digital archive? (yes, no, under which conditions?)

Table 1. Questionnaire.

Applicability and Practice of Quality Management Standards

When we had the results of the questionnaire to hand, we continued to analyse our pre-selected standards. Missions, tasks, and organisational forms of memory organisations as well as legal and financial constraints allowed us to determine the degree of applicability of QM standards more reliably. Therefore we had to develop a set of criteria in order to make the assessment of applicability transparent. For example, the size of an organisation or the extent of in-house software development determines the adequacy of quality standards. Of course, we also considered all the requirements and constraints concerning QM standards explicitly stated by memory organisations within the questionnaire and related discussions.

Realisation

Identifying Relevant Quality Management Standards

This section illustrates how we determined a set of QM standards that are potentially useful for trustworthy digital archives.

Obviously there are several similarities between issues addressed by quality management systems and the attributes required for trustworthy digital archives.

Assessing the trustworthiness of archives needs an holistic view of the system responsible for the preservation of information. QM Systems also emphasise that all components of an organisation must be considered in order to improve the quality of products, processes, and systems. Moreover, both approaches stress the need to investigate and respect customer needs. Therefore, we have taken generic and high-level QM standards into account.

Since the preservation of digital information is highly dependent on reliable IT-systems, we have also considered IT-specific standards dealing with the quality of IT on an organisational and management level.

Security is another indispensable attribute for the trustworthiness of archives. Therefore our study also includes standards that focus mainly on the management of security within IT-systems.

Additionally, there are many specific quality standards available. They generally concentrate on the distinct characteristics of products or processes, such as the operating and supplying conditions for storage media or devices. This category of standards is out of scope here, since they do not address quality management systems directly. But, of course, one of the tasks of a QM system is to implement and control processes that identify, assess, and apply such standards.

These considerations lead to an initial set of QM related standards that will be explored in more detail to check for applicability in practice.

Survey

The survey took place during June and July 2008 when the questionnaire was distributed as a PDF form and collected via email. The survey was restricted to Germany, because the financial- and time resources were very limited and the intention was to initiate national activities.

The participants had approximately three to four weeks in which to deliver the answers electronically or via fax.

Comparison of Theoretical and Practical Results

As third step we compared the more theoretical consideration with the answers from the survey. The goal was to investigate the usability of standards in practice and to figure out the hurdles that prevent institutions from effectively using standards. We wanted to find out the contexts of the standards and their portability into the area of long-term preservation.

First Results of the Study

Identified Quality Management Standards

Here we present some consituents of our set of identified standards and illustrate their potential usefulness for trustworthy archives.

Let us start with a glance at the popular ISO 9000 family. ISO 9000 (2000) describes fundamentals and introduces principles of quality management, which correspond in varying degrees to the principles and derived criteria as formulated in the *nestor* catalogue for trustworthy digitals archives. Documentation, internal and external transparency and adequacy are basic principles in this catalogue. For example, ISO's quality management principles stress customer focus, the process approach, and leadership. Leadership means to establish unity of purpose and direction of the organisation which leads to an adequate organisational structure. The process approach facilitates an integrated view to the long-term preservation of information. The customer focus corresponds primarily to the definition of the archive's designated community. The ISO standard also underpins the value of documentation. Documentation enables communication of intent, both internally and externally, and consistency of action, and it serves as a means of traceability. ISO 9000 (2000) also provides a consistent set of definitions for terms relating to quality management and introduces different types of documents used in the context of quality management. Based on the fundamentals of ISO 9000 (2000) another member of the family, namely ISO 9001 (2000), defines requirements for a quality management system where an organisation needs to demonstrate its ability to provide products that fulfil customer and applicable regulatory requirements and aims to enhance customer satisfaction. Document requirements include statements of a quality policy and quality objectives, a quality manual, procedures and records required by ISO 9001 (2000), and documents needed to ensure the effective planning, operation and control of its processes. The standard also includes requirements for the control of documents. The fulfilling of these requirements will lead to high degree of transparency. The principle of adequacy is supported by the determination of requirements related to products (here Information Packages according to OAIS) and the review of these requirements. Since ISO 9001 (2000) provides concrete requirements for a QM system, audits can be conducted internally (informally), or externally (formally) for certification. Audits are used to determine the extent to which these requirements are fulfilled. Guidance for auditing based on ISO 9001 (2000) can be found in ISO 19011 (2002). With the help of a certificate an organisation can contribute to external transparency and increase confidence in its capabilities.

In summary, ISO 9001 and 9001 address and elaborate on aspects of trustworthiness, in particular documentation, transparency, and adequacy. The use of these standards avoids the need to reinvent a complete QM system, which is explicitly required by the *nestor* catalogue. Moreover, the set of standards can serve as a solid basis for more specific ones. ISO/IEC 90003 (2004), for example, provides a well structured guideline for the application of ISO 9001 (2000) to computer software. Such a method prevents the repeated and expensive wording of basic concepts and supports a top down approach, which is suitable to manage and control the complexity and organisational heterogeneity of long-term preservation.

Maturity models are another category of standards that are useful for quality management. They define a set of attributes that allow the assessment of the maturity of an organisation to fulfil certain tasks. CMMI (Capability Maturity Model Integration) is a popular example, which has its origin in the evaluation of software subcontractors. CMMI now offers an extensive framework for process improvement and for benchmarking organisations mainly with the focus on development projects. Despite this project-orientated view, we have recognised useful concepts and elements. CMMI also considers cross-project organisational aspects and, like ISO 9000 (2000),

complies with the process-orientated approach. In particular, CMMI stresses the institutionalisation of processes and provides generic goals and practices for the management of processes, which includes, for example, the defining, planning, implementing, monitoring, and controlling of processes; planning of processes also covers the provision of adequate resources like funding, skilled people, or appropriate tools. CMMI additionally addresses a range of specific issues such as requirements development, requirements management, or risk management as well as process and product quality assurance. Since CMMI stresses the importance of requirements it supports the principle of adequacy. The standard also describes procedures for internal and external assessments, and the introduction of different maturity levels enables the continuous improvement.

In summary, CMMI extends and refines topics that are listed in the nestor catalogue. It is more detailed than ISO 9001 (2000)and additionally provides many practices. In our opinion it is particularly suitable for organisations that conduct large-scale projects like mass digitisation, migration of extensive collections, or ingests from many different information producers.

In our opinion information security, primarily in the area of digital information, is another prerequisite for trustworthiness. In contrast to safety, security also considers social and therefore organisational aspects as addresed in the nestor catalogue. Moreover, information security needs to be managed like quality and processes. Information is the core asset of an archive. Fortunately, we can refer to already existing standards especially to the ISO 27000 series. ISO 27000 (2009) specifies the fundamental principles, concepts, and vocabulary for the ISO 27000 series. ISO 27001 (2005) defines the requirements for an Information Security *Management* System (ISMS). ISO 27002 (2005) provides codes of practice, for example in the areas of security policies, organisation of information security, access control, information security incident management, and business continuity management. Procedures for certification and self assessment are also addressed by this series of standards.

Of course, we have to bear in mind that these potentially useful standards are not primarily designed for memory organisations or for digital long-term preservation. Their genericity, underlying design goals, or other reasons may constrain the practical applicability. On the other hand we are convinced that standards that concentrate very deeply on the details of long-term preservation are not suitable for providing an holistic framework for assessing the trustworthiness of memory organisations or any related service providers.

Survey Results

From 53 distributed questionnaires we received 18 responses that could seriously be considered for analysis. So this study cannot be regarded as highly representative and comprehensive. It has to be interpreted as a first step into a deeper analysis on the transferability of methods and standards from different economically more important and dominant branches to an economic niche: digital long-term preservation.

Nevertheless, we did receive important feedback from those who were simply not able to answer the questionnaire because they had not proceeded very far in establishing a digital archive. This was the case in one of the museums, where public body in charge of the museum had not yet recognised the preservation of the digital

assets as an important issue to save cultural heritage and therefore limited their financial contribution to the basic function of the museum. Our conclusion from this feedback is that quality management, as well as long-term preservation, has not yet reached public awareness and nor led to any action. Only a few stakeholders in long-term preservation have grasped the importance of standards for quality management, processes, and security for the preservation task so far.

88% of the institutions, who responded to the survey, were public bodies. Most (eight) of those belong to a university or research institution, five are libraries, four belong to public administrations, three are archives, and three data centres. We received only two responses from commercial institutions, although we asked 14.

Asked for the overall mission of their institution most of them identified the tasks preservation/conservation, provision and making objects accessible as key issues for their institution. Out of 18 institutions, ten have defined goals and policies for their digital archive and its operation, five of those have even published their policies, whereas two institutions have no policy in place and seven have only planned to compile a digital preservation policy.

To the question on the existence of a financial concept to the long-term provision of digital objects, 69% of the institutions gave a positive answer, 31% said they did not have one. However, "long-term" in this sense corresponds to time scales between two years (three institutions), three years (one institution), and five years (five institutions). Only one participant has a 10-year future financial concept in place.

Asked whether the existence of the digital archive could be established after structural changes in organisation, most responded that this concept and question were irrelevant for public administrations.

Another important response revealed that, primarily, 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, tranparency and quality control of ingested objects. An IT-concept as well as a security concept has been introduced into most of the institutions. Summarising the answers to those questions: 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.

Surpringsingly only two out of 16 institutions had appointed a quality manager.

Looking into the standards used, 12 institutions answered that they comply with standards, three do not. In detail it looks as follows:

ISO 9000 (2000)	1 (full)
ISO/IEC 20000[6]	1 (full)
ITIL[7]	3 (partially)
V-Modell[8]	2 (mostly)
MoReq[9]	1 (full) 1 (partially)
DOMEA[10]	2 (full) 1 (mostly) 1 (partially)
DINI Certificate[11]	5 (full) 1 (mostly) 2 (partially)
ISO 15408[12]	1 (partially)
BSI[13] Standard 100-3	1 (partially)
BSI [14] Grundschutzkatalog	2 (full) 2 (mostly) 2 (partially)
BSI Grundschutzzertifikat	1 (partially)

Table 2. Answers to the question about use of standards.

One essential part of the survey was the investigation of practices regarding digital archiving systems. As we anticipated, the majority, 13 out of 18 institutions, decided on a self-developed software solution (only 9 documented it). This fits into the overall picture that long-term preservation is always bound to a designated community and therefore to have very community-specific needs. Eight out of 15 answered that they use a service provider, either an external one with a private contract or an administrative contract, for software development, seven do not.

Another question looked into the quality management of the service provider. Here four institutions answered that their service provider performs quality management, one answered 'no' and five did not know that. Only one institution mentioned ITIL as standard in use at the service provider for software development.

The type of digital objects preserved by the institutions we interviewed varies from pure text formats via video and audio formats to software and interactive multimedia. In fact, a significant amount of objects has been collected, whose only chance of survival is to be maintained in a digital preservation archive using either migration or emulation as archiving methods in order to be available and interpretable in future.

[6] ISO/IEC 20000-1:2005. Information technology – Service management – Part 1: Specification: http://www.iso.org/iso/catalogue_detail?csnumber=41332
[7] ITIL Knowledge – Overview: http://www.itil.org/
[8] IT-Beauftragte der Bundesregierung - V-Modell XT: http://www.cio.bund.de/DE/IT-Methoden/V-Modell_XT/v-modell_xt_node.html
[9] MoReq2 homepage: http://www.moreq2.eu/
[10] DOMEA - Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang: http://www.cio.bund.de/cln_102/DE/IT-Methoden/DOMEA/domea_node.html
[11] Deutsche Initiative für Netzwerkinformation [DINI], 2007
[12] The ISO 15408 Toolkit: http://www.iso15408.net/
[13] BSI: Federal Office for Information Security: https://www.bsi.bund.de
[14] BSI: IT-Grundschutz: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

Regarding the selection process of objects, 13 participants stated that they had selection criteria in place, only 3 of them published. All of them document in one or another way formal arrangements with their producers, either in the form of legal regulations, frame contracts, formal license agreements or deposit contracts.

Most of the institutions (11 out of 15) have a policy in place for keeping or improving their relation to their producers.

Quality control of objects and metadata is carried out by 14 institutions, just one stated "no".

Looking into the usage aspects, most institutions know their user community and half of the institutions have already surveyed the specific demands of their user group. They use this information to provide user-group specific access to the digital objects. Quality can often be measured by user satisfaction. Six institutions stated that they measure the user satisfaction, 9 stated "no". Nearly one third of the participants had a policy in place to continuously improve the relationship with their users.

Regarding aspects such as infrastructure and security, 11 institutions answered to the question if they had already defined their process and organisational structures of their institution as follows: 11 institutions said, that they designed the processes and structures, three had specified them, five realised them, four had also published their processes and strcutures, one institution had even evaluated their processes and structures. 10 have even documented their structures, whereas 5 have no documentation.

The final two questions tested the readiness to certify themselves as a trustworthy digital archive. Here we received interesting answers. Most institutions declined to answer. They tie their willingness to become a certified trustworthy digital archive to the cost (time, effort and money) required to prepare themselves for the certification and fulfilment of the criteria and to the effective certification fees. This attitude differs from other communities, where, for example, an ISO 9000 (2000) certification is the basis for a successful business.

Conclusions of the Study

Assessing the Role of Management Standards in Actual Practice

Summarising the results, we see that the adoption of standards for quality management, processes and security as important factors in establishing trustworthy digital repositories has not yet reached in a large number of those institutions carrying out the duty of long term preservation. The results from the survey also indicate, that the participants of this study, generally speaking, recognise the high importance of those standards for their local institutions, but have problems in using those standards in practice. If they do use them, it is more in the sense of guidelines.

The problems arising while applying standards into new domains such as long-term preservation can be traced back to the heavy complexity of those standards that affect the understanding of the standards themselves in a negative way. Further reasons and potential solutions to the problem still need to be analysed in future studies.

The impression from the study leads to the finding that there is a certain interest in a specific standard covering all relevant aspects of a trustworthy digital repository, but at this time there is not yet a real need for using it as an instrument for quality control or for marketing.

Assessing the applicability of management standards

A closer look at the identified management standards has revealed that they are useful for assessing the trustworthiness of digital archives. Quality management standards as well as process and security management standards cover many concepts and topics that are already formulated as principles and criteria for trustworthiness. This holds especially for criteria that address the overall organisation of an archive, the processing of digital objects during the whole life cycle, and security issues too. The report of this study (Borghoff & Rödig, 2008) describes how *nestor*'s criteria and their underlying concepts relate to the topics of selected management standards. Due to the limited resources for this study we had no chance to elaborate a detailed mapping for every criteria and every identified standard. Nevertheless, we are convinced that we have enough evidence to show that an integration of management standards, in whichever form, leads to tangible advantages especially if a formal kind of assessment is the aim. On the other hand, several facts hamper easy integration. For example, referencing management standards as a whole or even major parts of them would cause unacceptable redundancies instead of providing consistent refinements. Moreover, the content of current management standards still overlaps. Concepts and techniques for tailoring to individual needs are not unified or are even missing. But those are important for handling the heterogenious amount of existing digital archives, which is also confirmed by several surveys. Finally, the landscape of standards and standardisation is a little confusing, but this study provides the first concise overview.

Applying management standards jointly with the nestor catalogue

The study discusses two basic alternatives to integrating the *nestor* catalogue and management standards beyond simple cases like reusing definitions of terms. The first alternative suggests the introduction of a management standard as a starting point and to redesign the *nestor* catalogue. General parts of the catalogue could then be covered by the management standard and long-term specific topics by the redesigned *nestor* catalogue. The heterogeneity of archives could be treated by further specialised standards or so-called technical reports, for example, if software is developed inhouse or if extended security measures are required due to legal restrictions. A life-cycle-orientated process management standard is a good choice for a top level standard because the *nestor* catalogue already reflects life cycles for digital objects as well as for archives. Moreover, this category of standards can serve as a framework for all the standards that are necessary to cover comprehensively the aspects a trustworthy archival system requires. Another option is to start with a quality management standard; the favoured one is ISO 9001 (2000), which is also based on the process-orientated concept. This modular alternative considers the complexity and heterogeneity of digital long-term preservation but requires at least two standards and, of course, efforts for redesigning the nestor catalogue and for determining the optimal management standard.

The second alternative leaves the basic structure and the abstract level of the *nestor* catalogue unchanged in essence. Integration requires the establishment of the appropriate sections of the *nestor* catalogue on the one hand, and of the management standards on the other. This approach is flexible because it enables a fine-grained adaptation to long-term specific topics. Of course, product and non-management process standards or parts of them can be referenced too. But problems will arise when the links should have a formal character, for example, for certifications. Then it is necessary, firstly, to synchronise the subsets over time, and secondly, to clarify whether the determined subsets fulfil the actual conformity rules, which are still quite restrictive. This problem would be less severe if the references were only informative (informal). Despite the shortcomings, this alternative may be preferred to the first one since there is no basic management standard required and the effort for redesigning the nestor catalogue, which is already fairly consolidated, is lower.

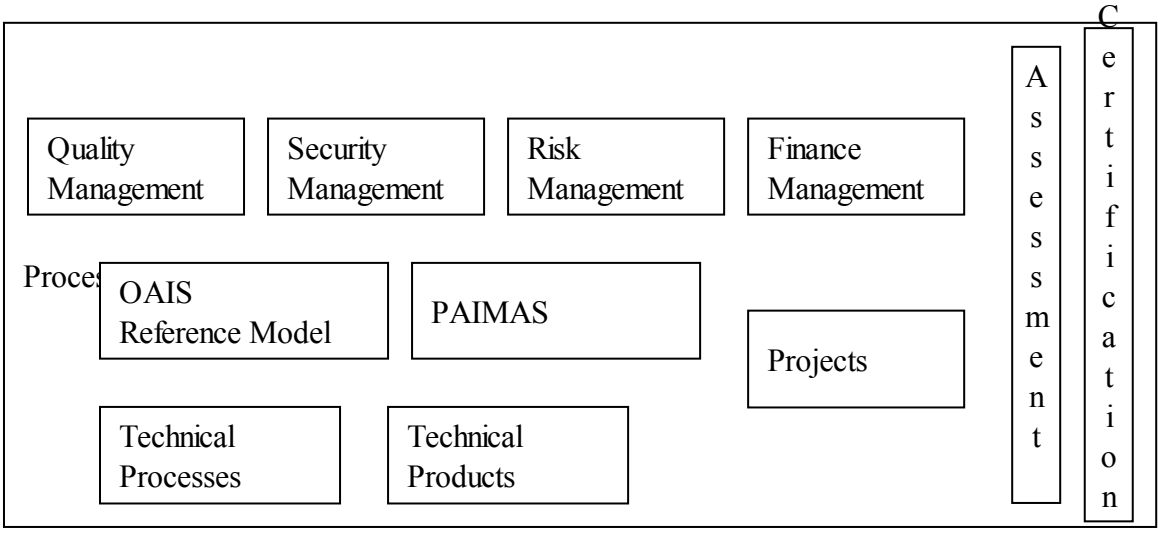

Figure 1. Fields for standardisation.

There are still more configurations and aspects to discuss; however, it is worthwhile to design an architecture that integrates management standards, in addition to other types of standards, as seamlessly as possible. Figure 1 illustrates the situation. Such integration facilitates the complete demonstration of the foundation of trustworthiness and soundness of an archival system, that is, transparency, adequacy, measurability, and documentation.

Further Issues and Work

Investigating certification procedures

For the development of an auditing or certification procedure for trustworthy digital archives, proven methods from different domains could be used. So within the INS2010 initiative we plan to conduct a study that identifies relevant certification methods and evaluates their usage within the digital long-term preservation domain.

The goals of this study are to initiate the development of a standardised certification framework that offers producers as well as consumers of digital objects transparency within the selection process of potential service providers or within the aquisition process of hard- and software.

Going back to certified organisations, processes and products in a standardised way may construct the approval of services or the aquisition of complex hard- and software systems more efficiently.

During the development, appraisal and introduction of auditing and certification procedures the following basic questions arise, which have to be answered within the scope of standardisation:

- How can one adequately document the compliance with criteria?
- How is the formal certification procedure designed?
- Which are the benefits produced for different partners?
- What ist the effort involved with a certification?

Developing the nestor catalogue

The *nestor*/DIN working Group will use the outcomes of this and the subsequent study during the standardisation process at DIN and will work out crosslinks to international approaches based on the idea of trustworthy digital archives.

In the long term, the establishment of a certfication process based upon the *nestor* criteria is planned.

References

Borghoff, Uwe M., and Rödig, P. (2008). *Schlussbericht zum Projekt INS 2008 - Teilprojekt Qualitätsmanagement für vertrauenswürdige digitale Archive*.

Bundesamt für Sicherheit in der Informationstechnik. (2005). *Common criteria for information technology security evaluation V 3.1R3* http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf

Deutsche Initiative für Netzwerkinformation. (2007). *DINI certificate document and publication services 2007*, Version 2.0, September 2006, from http://edoc.hu-berlin.de/series/dini-schriften/2006-3-en/PDF/3-en.pdf

DRAMBORA (2007). *Digital Curation Centre and DigitalPreservationEurope (2007): DCC and DPE digital repository audit method based on risk assessment, V1.0*. Retrieved February 28, 2007, from http://repositoryaudit.eu/download

ISO 9000. (2000). *Quality management systems – Fundamentals and vocabulary.*

ISO 9001. (2000). *Quality management systems – Requirements.*

ISO 19011. (2002). *Guidelines for quality and/or environmental management systems auditing*

ISO/IEC 27000. (2009). *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

ISO/IEC 27001. (2005). *Information technology – Security techniques – Information security management systems - Requirements*

ISO/IEC 27002. (2005). *Information technology – Security techniques – Code of practice for information security management.*

ISO/IEC 90003. (2004). *Software engineering – Guidelines for the application of ISO 9001:2000 to computer software.*

McGovern, N. Y., Kenney, A. R., Entlich, R., Kehoe, W. R. & Buckley, E. (2004). Virtual remote control: Building a preservation risk management toolbox for web resources, *D-Lib Magazine*, *10* (4). Retrieved June 19, 2009, from http://www.dlib.org/dlib/april04/mcgovern/04mcgovern.html

nestor Working Group on Trusted Repositories Certification. (2006, December). *Catalogue of criteria for trusted digital repositories* – Version 1 (Request for Public Comment). Frankfurt am Main. Retrieved June 19, 2009, from http://nbn-resolving.de/urn:nbn:de:0008-2006060703

OCLC and Center for Research Libraries. (2007, February). *Trustworthy Repositories Audit and Certification: Criteria and checklist*. Retrieved June 19, 2009, from http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf

OCLC/RLG-NARA Task Force on Digital Repository Certification, CLR, DCC, DPE and *nestor*. (2007). *Core requirements for digital archives (common principles)*. Retrieved June 11, 2010, from http://www.crl.edu/archiving-preservation/digital-archives/metrics-assessing-and-certifying/core-re

Open Archival Information System. (2003). *ISO14721:2003 Space data and information transfer systems – Open archival information system – Reference model*; see also Blue Book ISO 14721:2003 Issue 1

RLG Working Group on Digital Archive Attributes. (2002). *Trusted digital repositories: Attributes and responsibilities*. Mountain View CA. Retrieved June 19, 2009, from http://www.oclc.org/programs/ourwork/past/trustedrep/repositories.pdf

Task Force on Archiving Digital Information. (1996). *Preserving digital information, commission on preservation and access*. Washington D.C.