The Use of Quality Management Standards in Trustworthy Digital Archives

Susanne Dobratz*, Peter Rödig, Uwe M. Borghoff**, Björn Rätzke****, Astrid Schoger*****

*Humboldt-Universität zu Berlin, University Library
Unter den Linden 6
D-10099 Berlin
dobratz@cms.hu-berlin.de

**Universität der Bundeswehr München / University of the Federal Armed Forces Munich,
Werner-Heisenberg-Weg 39,
D-85579 Neubiberg
peter.roedig|
uwe.borghoff@unibw.de

***Bayerische Staatsbibliothek / Bavarian State Library
Ludwigstraße 16,
D-80539 München,
astrid.schoger@bsb-muenchen.de

****Rätzke IT-Service
Strasse 58 Nr. 10,
D-13125 Berlin,
bjoern@raetzke.org

Abstract

Quality management is one of the essential parts to become a trustworthy digital archive. T*he German network of expertise in Digital long-term preservation (nestor),* in cooperation with the *German Institute for Standards (DIN)* has undertaken a small study in order to systematically analyse the relevance und usage of quality management standards for long-term preservation and to filter out the specific standardisation need for digital archives. This paper summarises the first results of the study. It gives a first overview on the differences in understanding the task “quality management” amongst different organisations and how they carry out appropriate measures like documentation, transparency, adequacy, and measureability in order to demonstrate the trustworthiness of their digital archive.

1 Introduction

Already 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 ...*’ [11]. Some investigations in creating criteria and measuring the risk for a long-term preservation of digital objects have been carried out by several stakeholders, like the ‘*Cornell Library Virtual Remote Control Tool’* project of Cornell University[5], the ERPANET project[4], 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 led to increased conception and installation of digital archives during the last couple of 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 like ISO 9000 etc.

During the establishing of a DIN/ISO Working Group in Germany for defining criteria for trustworthy digital archives, the ostensible question on the recent degree of acceptance and usage of quality management standards within the cultural heritage sector (libraries, archives, museums) arose. Therefore the *German Institute for Standards (DIN)* sponsored a small study in order to systematically analyse the relevance und 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 amongst 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 kind in Germany: libraries, archives, data centres, publishers, museums.

1.1 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 endangered by the aging of storage media, the obsolescence of the underlying system, the application software as well as changes in the technical and organisational infrastructure. Malicious or erroneous human actions also put digital objects at risk. Trustworthy long-term preservation in digital repositories requires technical, as well as organisational provisions. 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 e.g. 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 of 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 provenience 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. Availability of objects is a central 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 trustworthy 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 fulfill 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 allows 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, backers, management, and employees. Parts of the documentation which are not suitable for the general public (e.g. company secrets, security-related information) can be restricted to a specified circle (e.g. certification agency). Transparency establishes trust, because it allows interested parties a 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 fulfillment of a certain criteria depends always on the designated community, it is not possible to create "hard" criteria for some of them, e.g. how can be measured, what adequate metadata is? Transparency also makes the indicators accessible for evaluation.

Recent research on trustworthy digital repositories

The ideas discussed in this paper are based on early developments on a framework describing requirements and functionalities for archiving systems that focus on the long-term preservation of digital materials, the Open Archival Information System (OAIS) [2]. 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 in 2002 [10] and finally released in February 2007, under the title: *Trustworthy Repositories Audit and Certification Checklist (TRAC)* [7], a checklist useable to conduct 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 allaborates the catalogue as guideline for the conception and design of a trustworthy digital archive [6]. 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 and developed an risk management tool for trusted digital long-term repositories, called *Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) in 2007*[3]. Within the PLANETS project[1], 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 agreed upon a set of so called common principles, ten basic characteristics of digital preservation archives [8].

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:

1. Is a new single standard for trustworthy digital archives needed?
2. How does this standard refer to existing standards?
3. Is an evaluation or even a certification of trustworthy digital archives desireable and useful?

1.2 Quality management (QM) and standards

Quality of products, processes, and systems is a key factor for economical success in an open world. Implementing and operating a quality management system is vital for many organisations in order to survive on the market. But also public administrations are interested in a more efficient and effective use of revenues resources for public services. Therefore numerous principles, methods, practices, and techniques have been developed in the last decades. Many of them are consolidated, broadly accepted and published in standards.

In order to get a first idea of core concepts we refer to the well known standard ISO 9000. 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 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.

2 Background and focus of this study

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

The present study analyses several quality management standards regarding their applicability for the evaluation of trustworthiness of digital archives. It extracts to which 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 nationally and internationally high attention.

While the amount of digital data explodes and an growing amount 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 operation of such archives.

Internationally there are two ways: first to define catalogues of criteria and second to work out risks potentials based on the specific goals of the considered archives. Thereby 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 towards standardisation and the efforts towards certification. The latter issue can only be carried out, if reliable standards, criteria, and most important, appropriate metrics 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 standards. Certification methods and schemas will be subject of a follow-up study in 2009.

[11] http://www.planets-project.eu

3 Methodology

3.1 Identification of relevant quality management standards

In a first step we identified and characterised 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 a first set of relevant standards. This first selection provides a reference in the questionnaire in order to find out easier which standards are concretely known, discussed, or already applied or refused. Moreover, this set of standards serves as a basis for a deeper analysis of the applicability of QM standards in long-term preservation considering the results of the questionnaire.

3.2 Survey of quality management standards used in long-term preservation

Second, 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. 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.

In addition, institutions that were known to work 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 asked: libries, libraries at universities, museums, archives (public bodies), archives (private, corporate bodies), and commercial vendors.

The design of the questionnaire should mirror some of the criteria in the nestor catalogue as well as make visible those activities that could be interpreted as quality management although they might not be recognised as such by the institution. We asked for the institution‘s characteristics as well as for the policy of the digital long-term preservation archive and the kind and amount of digital objects hold. Several specific questions focused on the use of standards and quality management.

The 44 questions were the following[2]:

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, …)[3]
10	Mission oft 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 archive granted after structural changes in organisation?
	Quality and security management
16	Quality management (yes, no)
17	Quality management: what is done precisely?
18	Do you have a quality manager?
19	Have you concerned about standards and norms?
20	Have you discussed standards and norms?
21	Has the applicability of standards been analysed in your institution?
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**
	Ingest
28	Types of objects (carrier, format, content)
29	Selection criteria (yes, no, planned, published)
30	Do you have formal regulations with producers?
31	Do you have a concept for keeping the quality in the relation with the producers?
32	Do you carry out quality control measures for objects and metadata?
	Access
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?

[2] Details and the whole questionnaire will be given in the final study report scheduled for November 2009.

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

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?)

3.3 Applicability and practise of quality management standards

Having the results of the questionnaire at hand we can continue to analyse our pre-selected standards. Missions, tasks, and organisational forms of memory organisations as well as legal and financial constraints will allow us to determine the degree of applicability of QM standards more reliantly. Therefore we have 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 additionally consider all requirements and constraints concerning QM standards explicitly stated by memory organisations within the questionnaire and related discussions.

4 Realisation

4.1 Identifying relevant quality management standards

This section illustrates how we have determined a first set of QM standards 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 a holistic view on the system responsible for the preservation of information. QM Systems also underpin that all components of an organisation have to be considered in order to improve quality of products, processes, and systems. Moreover, both approaches emphasise the task 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.

Moreover, security is another indispensable attribute for the trustworthiness of archives. Therefore our study also comprises standards that are mainly focussing on the management of IT-systems security.

Additionally, there are many specific quality standards available. They generally concentrate on distinct characteristics of products or processes like the operating and stocking 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 it is one of the task of a QM system to implement and control processes that identify, assess, and apply such standards.

This considerations lead to a first set of QM related standards that will be investigated in more detail in order to check for applicability in practised.

4.2 Survey

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

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

4.3 Comparison of theoretical and practical results

As third step we will compare the more theoretical considerations with the answers from the survey. Since this step is still work in progress, we can only state the basic findings in this paper so far. The final report of the study is scheduled for the end of November 2008.

The goal is to investigate the usability of standards in practise and to figure out the hurdles that prevent institutions to effectively use standards. We want to find out the contexts of the standards and their portability into the area of long-term preservation.

5 First results of the study

5.1 Identified quality management standards[4]

Here we present some members 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 describes fundamentals and introduces principles of quality management, which correspond to the principles and derived criteria as formulated in the nestor catalogue for trustworthy digitals archives in varying degrees. Documentation, internal and external transparency and adequacy are basic principles in this catalogue. For example, ISO's quality management principles stress the 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 form. The process approach facilitates an integrated view to the long-term preservation of information. The costumer 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

[4] A first report for this phase of the study is scheduled for the end of August.

internally and externally, and consistency of action, and it serves as a mean of traceability. ISO 9000 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 another member of the family, namely ISO 9001, 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. Audits are used to determine the extent to which these requirements are fulfilled. Audits can be conducted internally or externally (formal and informal). Guidance for auditing can be found in ISO 19011. With the help of a certificate an organisation can contribute to external transparency and increase confidence in its capabilities.

Maturity models are another category of standards that are useful for quality management. They define a set of attributes that facilitate to find out the maturity of an organisation to fulfil certain tasks. CMMI (Capability Maturity Model Integration)[5] 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 oriented view, we have recognised useful concepts and elements. CMMI also considers cross-project organisational aspects and, like ISO 9000, complies with the process oriented approach. Especially, CMMI stresses the institutionalisation of processes and provides generic goals and practices for the management of processes, which includes for example 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 like requirements development, requirements management, or risk management as well as process and product quality assurance. CMMI also describes procedures for internal and external assessments.

Information security, primarily in the area of digital information, is another prerequisite for trustworthiness. Information security needs to be managed like quality and processes. Information is the core product of an archive. Fortunately, we can refer to already existing standards especially to the ISO 27000 series. ISO 27000 (still under development) specifies the fundamental principles, concepts, and vocabulary for the ISO 27000 series. ISO 27001 defines the requirements for an Information Security Management System (ISMS). ISO 27002 provides code of practices, 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 and for digital long-term preservation. Their generosity, underlying design goals, or other reasons may constrain the practical applicability. The last phase of this study will cover this issue.

5.2 Survey results

From 53 distributed questionnaires we received 17 answers 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, well knowing of it's raising importance.

Nevertheless, we did receive important feedback from those who where simply not able to answer the questionnaire because they had not proceeded very far in establishing a digital archive. This was the case especially in one of the museums we asked, where the superior organisation, the public body in charge of the museum, has not yet recognised a preservation of the digital assets as an important issue to save cultural heritage and therefore limited the 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 reached public awareness and led to action yet. Only few stakeholders in long-term preservation have perceived the importance of standards for quality management, processes, and security for the preservation task so far.

15 out of 17 institutions were public bodies. Most (7) of those belong to a university or research institution, 5 are libraries, 4 belong to an administration, 3 are archives, and 3 data centres. We received only 2 responses from commercial institutions, although we asked 14 .

Asked for the superior mission of their institution most of them identified the tasks preservation/conservation, provision and making objects acessible as key issues for their institution. From 17 institutions, 9 have defined goals and policies for their digital archive and its operation, 5 of those have even published their policies, whereas 2 institutions have no policy in place and 7 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, 10 institutions gave a positive answer, 5 denied to have one. However, long-term in this sense corresponds to time scales between 2 years (3 institutions), 3 years (1 institution), and 5 years (5 institutions). Only one participant has a 10 year future financial concept in place.

Asked, how can the existence of the digital archive be granted after structural changes in organisation, most answers argued that this concept and question are irrelevant for public administration.

Another important response revealed, that primarily public body institutions didn't recognise an advantage for themselves, their services, and customers in being

[5] http://www.sei.cmu.edu/cmmi

certified for ISO 9000 or even as trustworthy digital archive. The portability of quality management standards to the procedures and services in public administration is considered as hardly possible. Often the enormous complexity of standards is seen as main barrier to comply with them completely. Instead, standards are (mis-)used as guidelines and their principles applied to selected workflows and processes: documentation, tranparency, 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 mirrored a strong demand for deeper and broader information on standards as well as support and training during the introduction of standards.

Surprisingly only 2 out of 16 institutions had appointed a quality manager.

Looking into the standards used, 12 institutions answered that they comply with standards, 3 don't. In detail it looks as follows:

ISO 9000	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]	1 (full) 2 (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)

One essential part of the survey was the investigation of habits regarding digital archiving systems. As we anticipated, most, 13 out of 17, institutions decided for 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 very community specific needs. 8 out of 15 answered to use a service provider, either an external with a private contract or an administrative contract, for software development, 7 don't.

Another question looked into quality management of the service provider. Here 4 institutions answered that their service provider perform a quality management, 1 answered 'no' and 5 didn't know that. Only 1 institution mentioned ITIL as standard in use at the service provider for software development.

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

Regarding the selection process of objects 13 participants stated to have 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 form of legal regulations, frame contracts, formal license agreements or deposit contracts.

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

A quality control of objects and metadata is carried out by 14 institutions, just 1 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 it to provide user group specific access to the digital objects. Quality can often be measured by measuring the satisfaction of the users. 6 institutions stated to measure the user satisfaction, 9 stated 'no'. Nearly one third (5) of the participants have a concept in place to continuously improve the relationship to their users.

Regarding aspects like infrastructure and security, 11 institutions stated to the question if they had defined the process and organisational structures of their institution:
11 designed, 3 specified, 5 realised, 4 published, 1 evaluated. 10 have even documented their structures, whereas 5 have no documentation.

The last two questions tested the readiness to certify themselves as trustworthy digital archive. Here we received interesting answers. Most institutions refused to answer 'yes' or 'no'. Their willingness to become a certified trustworthy digital archive strongly depends on the costs (time, effort, and money) for preparing and conduction the certification. This attitude differs from that in

[6] http://www.iso.org/iso/catalogue_detail?csnumber=41332

[7] See http://www.itil.org

[8] Please refer to KBSt at http://www.kbst.bund.de

[9] http://www.moreq2.eu

[10] See KBSt: Federal Government Co-ordination and Advisory Agency

[11] See www.dini.de [21]

[12] See http://www.iso15408.net

[13] BSI : Federal Office for Information Security

[14] See http://www.bsi.bund.de/english/topics/topics.htm

different communities where e.g. an ISO 9000 certification is the basis for a successful business.

First conclusions

Summarising the first results, we regard the adoption of standards for managing quality, processes, and security as an important factor to establish trustworthy digital archives. The first results from the survey indicate that also the participants of this study, generally spoken, see the high importance of such standards for their local institutions. We also recognized severe problems in using those standards in practice. Apparently standards are applied mostly in the sense of guidelines.

The problems arising while transferring standards into new domains like long-term preservation can be traced back to the heavy complexity of those standards that affect the understanding of the standards itself in a negative way. Further reasons and potential solutions to the problem have still to be analysed in the final part of this study.

The first impression from the study leads to the finding that there is a need for a specific standard covering all relevant aspects of a trustworthy digital repository.

References

[1] Bundesamt für Sicherheit in der Informationstechnik (2005): Common Criteria V 2.3.

[2] ISO14721:2003 Space data and information transfer systems – Open archival information system – Reference model; see also Blue Book: http://www.ccsds.org/docu/dscgi/ds.py/Get/File-143/650x0b1.pdf

[3] Digital Curation Centre und Digital Preservation Europe (2007): DCC and DPE Digital Repository Audit Method Based on Risk Assessment, V1.0.: http://repositoryaudit.eu/download

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

[5] McGovern, Nancy Y.; Kenney, Anne R.; Entlich, Richard; Kehoe, William R. und Buckley, Ellie (2004): Virtual Remote Control: Building a Preservation Risk Management Toolbox for Web Resources, D-Lib Magazine 10 (4).: http://www.dlib.org/dlib/april04/mcgovern/04mcgovern.html

[6] nestor Working Group on Trusted Repositories Certification (2006): Criteria for Trusted Digital Long-Term Preservation Repositories – Version 1 (Request for Public Comment) English Version, Frankfurt am Main.: http://nbn-resolving.de/urn:nbn:de:0008-2006060703

[7] OCLC und Center for Research Libraries (2007): Trustworthy Repositories Audit and Certification: Criteria and Checklist. : http://www.crl.edu/PDF/trac.pdf

[8] OCLC/RLG-NARA Task Force on Digital Repository Certification; CLR; DCC; DPE und nestor (2007): Core Requirements for digital Archives (Common Principles). : http://www.crl.edu/content.asp?l1=13&l2=58&l3=162&l4=92

[9] RLG NARA Task Force on Digital Repository Certification (2005): Audit Checklist for Certifying Digital Repositories, RLG, NARA Task Force on Digital Repository Certification, Mountain View, CA.

[10] RLG Working Group on Digital Archive Attributes (2002): Trusted Digital Repositories: Attributes and Responsibilities, RLG; OCLC, Mountain View CA.: http://www.rlg.org/longterm/repositories.pdf

[11] Task Force on Archiving Digital Information (1996): Preserving Digital Information, Commission on Preservation and Access, Washington D.C.

[12] ISO 9000:2000 Quality management systems – Fundamentals and vocabulary

[13] ISO 9000:2005 Quality management systems – Fundamentals and vocabulary

[14] ISO 9001:2000 Quality management systems – Requirements

[15] ISO 19011:2002 Guidelines for quality and/or environmental management systems auditing

[16] ISO/IEC FCD 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary

[19] ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements

[20] ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management

[21] Deutsche Initiative für Netzwerkinformation: DINI Certificate Document and Publication Services 2007 [Version 2.0, September 2006]: http://edoc.hu-berlin.de/series/dini-schriften/2006-3-en/PDF/3-en.pdf