



Project no. 033572

CASPAR

Cultural, Artistic and Scientific knowledge for Preservation, Access and Retrieval

Instrument: Information Society Technologies

Thematic Priority: 2.5.10 Access to and preservation of cultural and scientific resources

REPORT ON TRUSTED DIGITAL REPOSITORIES



| | |
|----------------------|--------------------------------|
| Document identifier: | CASPAR-1203-RP-0101-1_0 |
| Submission Date: | 15-01-2009 |
| Due date: | 31-12-2008 |
| Work package: | 1200 |
| Partners: | All Partners |
| WP Lead Partner: | UG |
| Document status | FINAL |

Abstract: This document outlines important aspects of trust with respect to digital repositories, and the activities and standards which are important in engendering such trust.



Delivery Type Report
Author(s) CASPAR Consortium

Approval David Giaretta

Summary

Keyword List

Availability PUBLIC

Document Status Sheet

| Issue | Date | Comment | Author |
|-------|---------------|-------------------------------|--------------------------------|
| 0_0 | 15 April 2008 | Initial agreement on contents | David Giaretta, Candida Fenton |
| 0_1 | 01 Dec 2008 | Initial version | Candida Fenton |
| 0_2 | 12 Jan 2009 | Revised version | Joy Davidson |
| 1_0 | 14 Jan 2009 | Final version | David Giaretta |
| | | | |
| | | | |
| | | | |
| | | | |





Project information

| | |
|------------------------|---|
| Project acronym: | CASPAR |
| Project full title: | Cultural, Artistic and Scientific knowledge for Preservation, Access and Retrieval |
| Proposal/Contract no.: | IST-2006-033572 |

Project Officer: Carlos Oliveira

| | |
|----------|---|
| Address: | INFSO-E3 Information Society and Media Directorate General Content - Learning and Cultural Heritage Postal mail: Bâtiment Jean Monnet (EUFO 1167) Rue Alcide De Gasperi / L-2920 Luxembourg Office address: EUROFORUM Building - EUFO 1167 10, rue Robert Stumper / L-2557 Gasperich / Luxembourg |
| Phone: | +352 4301 33052 |
| Fax: | +352 4301 33190 |
| Mobile: | |
| E-mail: | Carlos.Oliveira@ec.europa.eu |

Project Co-ordinator: David Giarretta

| | |
|----------|---|
| Address: | STFC (formerly STFC), Rutherford Appleton Laboratory Chilton, Didcot, Oxon OX11 0QX, UK |
| Phone: | +44 1235 446235 |
| Fax: | +44 1235 446362 |
| Mobile: | +44 (0) 7770326304 |
| E-mail: | d.i.giarretta@rl.ac.uk |





CONTENT

| | | |
|-----------|--|-----------|
| 1 | INTRODUCTION | 5 |
| 1.1 | TRUST RELATIONSHIPS | 6 |
| 1.2 | HOW TO ENGENDER TRUST | 6 |
| 2 | CONCEPT OF TRUST | 8 |
| 2.1 | DEFINITIONS | 8 |
| 2.2 | PHILOSOPHY | 8 |
| 2.3 | SOCIOLOGY..... | 9 |
| 2.4 | THESAURI..... | 9 |
| 2.5 | ECONOMICS | 9 |
| 3 | APPROACHES TO TRUST | 11 |
| 3.1 | TYPES OF TRUST | 11 |
| 3.2 | POTENTIAL INTEREST GROUPS | 12 |
| 3.3 | FUNDING..... | 12 |
| 3.4 | DISTRIBUTED NETWORK | 12 |
| 3.5 | TRUST EQUATION..... | 13 |
| 4 | QUESTIONNAIRE | 14 |
| 4.1 | INTRODUCTION | 14 |
| 4.2 | RESPONDENTS | 14 |
| 4.3 | REPOSITORIES..... | 15 |
| 4.4 | FULL QUESTIONNAIRE RESPONSES | 18 |
| 4.5 | CONCLUSIONS FROM THE SURVEY | 28 |
| 5 | STANDARDS..... | 29 |
| 5.1 | INTRODUCTION | 29 |
| 5.2 | OVERVIEW OF RELEVANT ISO STANDARDS | 29 |
| 5.3 | OTHER RELEVANT STANDARDS..... | 31 |
| 6 | STANDARD AND CERTIFICATION | 34 |
| 6.1 | TYPES OF ACCREDITATION | 35 |
| 6.2 | HOW ARE ACCREDITATION BODIES SET UP? | 35 |
| 7 | REFERENCES | 37 |
| 8 | BIBLIOGRAPHY | 38 |
| A. | APPENDIX 1..... | 49 |





1 INTRODUCTION

Digital preservation refers to the series of managed activities necessary to ensure continued understandability and use of, and access to, digital materials for as long as necessary, regardless of technological, legal, cultural and social change. Such changes are difficult to predict and anticipating such changes and finding solutions to them is a challenging task. As digital preservation is a relatively new activity, digital repositories which undertake digital preservation can rarely provide evidence that they have preserved digital objects successfully through technological, legal, cultural and social change. This begs the question why should those with digital objects they wish to preserve, trust a repository to effectively preserve them over time?

There are a number of factors identified which make digital preservation more challenging than paper preservation, such as the ease of copying and modification of digital records which are seen as advantages of digital media but which are a liability when it comes to preservation. A digital object is not an object as it cannot 'speak' to a human without some technology in between, unlike writing on paper. Another factor is the need active management of digital media otherwise material will become inaccessible, and that digital objects need to be 'fixed' along with their technological infrastructure.

The Preserving Digital Information report of the Task Force on Archiving of Digital Information (Garrett & Waters, 1996) declared,

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

The issue of certification, and how to evaluate trust into the future, as opposed to a relatively temporary trust which may be more simply tested, has been a recurring request, repeated in many subsequent studies and workshops.

The *Reference Model for an Open Archival Information System* (OAIS, ISO 14721:2003), is now adopted as the "de facto" standard for building digital archives (NSF, 2007). Section 1.5 of OAIS (Road map for development of related standards) included an item for accreditation of archives, reflecting the long-standing demand for a standard against which Repositories of digital information may be audited and on which an international accreditation and certification process may be based. It was agreed that RLG and NARA take a lead on this follow-on standard. This they did, forming a closed panel which produced Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC, 2007).

TRAC was based on two documents, namely the OAIS Reference Model (OAIS, 2002) and the Report on Trusted Digital Repositories: Attributes and Responsibilities (RLG-OCLC, 2002). The former lays out fundamental requirements for preservation, while the latter focussed on the administrative, financial and organisational requirements for the body undertaking the preservation activities, and defined a trusted digital repository as

'one whose mission is to provide reliable, long term access to managed digital resources to its designated community, now and in the future'

Other, separate, work includes the nestor Catalogue of Criteria for Trusted Digital Long-term Repositories (nestor, 2006), which is also based on OAIS.

An OAIS is a specific type of digital repository defined in ISO 14721:2003. *Reference Model for an Open Archival Information System (OAIS)*. An OAIS preserves information and makes it available for a Designated Community, and the Designated Community must therefore trust that the OAIS will effectively preserve their digital information or objects.

CASPAR is a project which researches, implements, and disseminates innovative solutions for digital preservation based on the OAIS reference model. This report aims to examine ideas of



trust and their relevance to digital preservation repositories - specifically the CASPAR project. One of the aims of CASPAR (p 9 Conceptual Model) is

‘an increase in the trustworthiness of archives using CASPAR’.

Trust is therefore a central concept for the CASPAR project, and CASPAR consortium members are key players in many of the activities described in this document.

1.1 TRUST RELATIONSHIPS

Trust can be looked at in relation to a variety of activities undertaken by the CAPSAR project, and trust relationships between various stake holders will be explored. Trust relationships exist between an OAIS and external stakeholders including the Designated Community, funders of an OAIS, those submitting material to an OAIS, those accessing material held in an OAIS, other OAIS, the larger subject community and the digital preservation community as a whole. A further trust relationship occurs between an OAIS and any bodies providing services to it, such as a Representation Information Repository.

Within an OAIS there are trust relationships through the whole chain of custody, and these are tied up with ideas of reliability and authenticity. These include the trust relationship between a producer and a SIP (Submission Information Package) which is to do with reliability, and between a SIP and the subsequent AIP (Archival Information Package) and the subsequent DIP (Dissemination Information Package) and the DIP and the consumer, which are concerned with authenticity. There are also trust relationships between the entities of an OAIS such as those between:

- Ingest and Data Management
- Ingest and Archival Storage
- Data Management and Access
- Archival Storage and Access
- Preservation Planning and Administration
- Administration and Ingest, Preservation Planning, Archival Storage, Data Management and Access.

If any one of these links in the chain of trust relationships within an OAIS is broken, trust in the entire chain of custody is also broken.

As trust is something which does not exist in isolation but is a type of relationship between various participants, developing agreed standards and best practice within the preservation community are valuable activities to engender trust.

In what follows, for simplicity, we use the Designated Community to identify the ones whom we need to do the trusting.

1.2 HOW TO ENGENDER TRUST

For a digital repository to be considered trustworthy of undertaking long term preservation of digital objects, it must consider and address technical, legal and organisational issues.

The initial problem is how to persuade Designated Communities to trust a digital repository to do what it claims it will do. Users of systems and services are usually persuaded to trust a supplier by the provision of evidence that they have already supplied their services to another successfully. A track record has been established and testimonials from satisfied customers are available. The problem with digital preservation is that it has not yet happened, at least not over a very long period of time. A further problem for CASPAR is how to maintain trust between the designated communities and a repository over time, as the designated communities change over time.

Traditional archives which already have a body of users who trust them to preserve paper based material (as they have successfully done this already), are therefore in a good position to establish trusted digital repositories. However, a crucial difference between traditional archives



and digital repositories is that although paper can suffer benign neglect and be left on a shelf and still be accessible in one hundred years time, the same does not apply to digital information. Changes in storage media, hardware, software, file formats and other aspects of digital information make it unlikely that users will be able to understand, use and access unmanaged digital information successfully in the future. Digital objects therefore have to undergo active management for them to be accessible in the future, and whether documents will retain their authenticity during management processes is a key issue. Users of an OAIS therefore have to trust that those undertaking preservation activities can maintain the authenticity of the digital objects, which is a much more complex undertaking than for paper records.

Digital preservation is a relatively new domain, as addressing the problems of how difficult it can be to access, understand and use older digital information has only been really attempted in the last decade or so. There are therefore no track records of OAIS having successfully undertaken digital preservation over a significant time period, thus making the establishment of trust with potential users difficult. In addition it is impossible to be certain of future circumstances and technologies, making credible assurances of future situations difficult to give.



2 CONCEPT OF TRUST

Trust is a concept which has different meaning within different contexts, and therefore a variety of different definitions are available. There is no consensus across disciplines as to a definition of trust, and therefore to get an overview of the concept definitions from a number of disciplines have to be examined.

2.1 DEFINITIONS

The first definitions here comes from “The Oxford Dictionary of English” (2nd edition revised)

Noun

“Firm belief in the reliability, truth, or ability of someone or something”

“Acceptance of the truth of a statement without evidence or investigation”

Verb

“To believe in the reliability, truth, or ability of” (1)

(1) "trust *noun*" *The Oxford Dictionary of English* (revised edition). Ed. Catherine Soanes and Angus Stevenson. Oxford University Press, 2005. *Oxford Reference Online*. Oxford University Press.

2.2 PHILOSOPHY

Trust is also a concept that philosophy is concerned with, and the “Oxford Dictionary of Philosophy” has the following definition;

“trust: The attitude of expecting good performance from another party, whether in terms of loyalty, goodwill, truth, or promises. The importance of trust as a kind of invisible glue that binds society together is most visible when it is lost. Trust involves an element of risk, and epistemologists can have trouble categorizing it as rational, since it works best in advance, for example to motivate performance on occasions when defection may be to the advantage of the person trusted. Economically trust is precious, enabling parties to bypass the costly precautions and safeguards needed in transactions with parties whom one does not trust. Trustworthiness is a virtue, subsuming varieties such as truthfulness and fidelity. It is a general ambition of democratic politicians to be trusted whether or not they are trustworthy. (2)

(2) "trust" *The Oxford Dictionary of Philosophy*. Simon Blackburn. Oxford University Press, 2008. *Oxford Reference Online*. Oxford University Press.

Whilst the Oxford Companion to Philosophy has the following definition

“trust. Whether one trusts a specific other commonly depends on whether one thinks the other is trustworthy in the relevant circumstances. This depends on what knowledge one has of the other's future commitments to behave as one trusts. Some writers treat trust as a matter of rational assessment and rational choice on the parts of both the truster and the trusted. Perhaps because of its relation to trustworthiness, some theorists treat trust as inherently normative—even to the point of assigning an obligation of trustworthiness to one who is trusted. John Locke thought trust central to consensual government. Contrary to the purely rational-choice vision, many theorists suppose that only a normative commitment to some degree of trustworthiness can explain the success of many institutions and organizations in serving their clientele. “



Prof. Russell Hardin "trust" *The Oxford Companion to Philosophy*. Oxford University Press 2005. Oxford Reference Online. Oxford University Press.

The philosophical approach therefore relates the concept of trust to other concepts such as risk, truthfulness and expectation, and raises the key point that trust is most visible when lost.

2.3 SOCIOLOGY

Sociology is another subject area where trust is of importance and there is a definition from the "A Dictionary of Sociology" as follows

"Trust and distrust. A strong tradition in sociology argues that stable collective life must be based on more than mere calculations of self-interest and that, even in a business situation, an element of trust is essential. Émile Durkheim's celebrated phrase that 'in a contract not everything is contractual' states this position most succinctly.

One of the most influential recent discussions of trust (A. Giddens, *The Consequences of Modernity*, 1990) defines it as 'confidence in the reliability of a person or system' and provides a useful summary of the chief issues which are raised by this concept." (3)

(3) "trust and distrust" *A Dictionary of Sociology*. John Scott and Gordon Marshall. Oxford University Press 2005. *Oxford Reference Online*. Oxford University Press.

2.4 THESAURI

As trust is a concept important in many spheres, in order to understand it more fully, it is useful to look at terms with similar meaning as indicated in thesauri such as "The Oxford Paperback Thesaurus" which lists related terms as

"Confidence, belief, faith, certainty, assurance, conviction; reliance."(4)

(4) "trust noun" *The Oxford Paperback Thesaurus*. Ed. Maurice Waite. Oxford University Press, 2006. *Oxford Reference Online*. Oxford University Press.

Roget's 21st Century Thesaurus, (Third Edition) defines trust as

"Belief in something as true, trustworthy"

and lists synonyms as

"Assurance, certainty, certitude, confidence, conviction, credence, credit, dependence, entrustment, expectation, faith, gospel truth, hope, positiveness, reliance, stock, store, sureness" (5)

(5) *Roget's 21st Century Thesaurus, Third Edition* by Barbara Ann Kipfer

2.5 ECONOMICS

Economics is a further field where trust is an important concept, although it has a different meaning from the other subject areas discussed here. However, in the context of digital repositories where digital objects are deposited in a repository and maintained by repository staff, it is useful. The "A Dictionary of Economics" defines trust as

"Trust. An arrangement through which one set of people, the trustees, are the legal owners of property which is administered in the interests of another set, the beneficiaries." (6)

(6) "trust" *A Dictionary of Economics*. John Black. Oxford University Press, 2002. *Oxford Reference Online*. Oxford University Press. University of Glasgow. 16 October 2008

A final non-dictionary definition come from Seadle and Greifeneder



“trust — essentially a bet on future outcomes”(7)

(7) Seadle, M & Greifeneder, E “In archiving we trust: Results from a workshop at Humboldt University in Berlin” First Monday, Volume 13 Number 1 - 7 January 2008 <http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2089/1923>

This situation is summed up by Holland, who states that

“There are multiple definitions of trust and a single, simple definition is insufficient to capture the essence of the concept.” (8)

(8) Holland, C “Business Trust and the Formation of Virtual Organizations “1998. Proceedings of the Thirty-First Hawaii International Conference on System Sciences, v. 6: 602-10.

Trust is therefore an important concept in many subject areas with a range of definitions. Related concepts include reliability, truth, risk, expectation, confidence, and these are all relevant concepts when considering the activities of digital preservation.

A significant property of trust is that it is difficult to engender yet easy to destroy, and once lost is difficult to re-establish.



3 APPROACHES TO TRUST

3.1 TYPES OF TRUST

As well as there being different meanings of trust in different subject areas, different types of trust have also been identified by Jeffries (the Journal of Behavioral and Applied Management – Winter 2002 – Vol. 3(2) Page 129 “Subjective Norms, Dispositional Trust, and Initial Trust Development” Francis L. Jeffries).

Dispositional trust is to do with generalised expectations of the outcome of a situation, and it is operational when a decision to trust or not to trust is made in the absence of direct evidence as to whether another is or is not trustworthy. Dispositional trust is therefore to do with the nature of the trustor, or the one who is placing trust in another. Dispositional trust is believed to have an influence on the trustor’s interpretation of the behaviour of others and the cues the trustor attends to in situations involving trust

A second type of trust that has been identified is situational trust and this is trust in relation to a particular situation, and is therefore concerned with both trustor and trustee.

There are two key types of trust relationship that can be considered when examining trust in relation to digital preservation. First, is the trust relationship between the Designated Community and the repository as an organisation, and secondly is the trust relationship between the Designated Community and the digital objects held by the repository.

There are a number of properties of digital objects which a preservation repository must maintain if it is to retain the trust of its Designated Community.

1) Reliability: is related to the first creation of a digital object and can be considered as the trustworthiness of a resource, as a statement of fact, based on the author’s competence and the control on the genesis of the resource itself. Reliability is the responsibility of the creator of a digital object.

2) Authenticity: is a quality of the resource itself. An authentic resource is one that has not been tampered with or otherwise corrupted, based on identity and integrity. The authenticity of a digital object is the responsibility of the custodian or repository.

OAIS (revised) defines Authenticity as: the degree to which a person (or system) may regard an object as what it is purported to be. The degree of Authenticity is judged on the basis of evidence.

3) Accuracy: is related to the capability to control the intellectual content of an object during its whole life-cycle and use. Accuracy concerns the correctness and precision of content, based on the competence of the author and the controls on the process by which data are recorded and transmitted through space i.e., between persons, systems or applications and time i.e., when stored off line, or when the hardware or software is upgraded or replaced.

Dobratz states that

“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.” (9)

Dobratz, Susanne and Schoger, Astrid “Trustworthy Digital Long-Term Repositories: The nestor Approach in the Context of International Developments” in, L. Kovács, N. Fuhr, and C. Meghini (Eds.): ECDL 2007, LNCS 4675, pp. 210–222, 2007



3.2 POTENTIAL INTEREST GROUPS

There are a number of groups with an interest in the trustworthiness of digital repositories

- Repository users who want access to trustworthy information – today and in the future
- Data producers and content providers for whom trustworthiness provides a means of quality assurance when choosing service providers
- Resource allocators, funding agencies and other institutions that need to make funding and granting decisions
- Long term digital repositories that want to gain trustworthiness and demonstrate this to the public either to fulfil legal requirements or to survive in the market place

3.3 FUNDING

Trust is the one inescapable issue in archiving of any sort. Archiving materials for the next 100 years represents a bet on a future well beyond our own lifetime. Business models matter in any trust calculation. An archiving system that goes out of business could hardly be called reliable. At best bankruptcy freezes development and forces customers to shift platforms, and at worst it puts the content at risk. Today's funding models for long term archiving vary widely, and in times of fiscal pressure the political will to fund archiving may weaken.

Clearly no organisation or project can guarantee its own longevity. It therefore makes sense to think in terms of a chain of responsibility, where each organisation needs to be sure that its holdings are able to survive the organisation's demise. This could for example involve a formal handing over of its holdings, with all appropriate associated information, to a successor repository just before its demise. Alternatively the "initial" repository and its successor could have a significant overlap in existence. A special case of the latter is the distributed network of repositories.

3.4 DISTRIBUTED NETWORK

A distributed network may be used as a tool for digital preservation. The distributed network is a model which has become pervasive, and is now being applied as a key element of digital preservation strategy. A distributed network of digital repositories is less vulnerable to many of the challenges digital preservation faces, than a standalone repository. This sees the advent of 'distributed digital preservation federations' which are geographically distributed institutions who are banding together to form solutions to digital preservation problems. (Walters, Tyler)

In this situation a high level of trust must be engendered between the institutions developing the network, and Tyler Walters expresses this as

'Trust means that we rely upon the organisations or institutions maintaining the digital libraries or archives to sustain the information deposited in it, and that this information remains authentic and reliable, and unchanged over time and across technologies' (10)

(10) Walters, Tyler "Creating trust relationships for distributed digital preservation federations", in, ipres 2008 proceedings of the fifth international conference on digital preservation of digital objects: joined up and working: tools and methods for digital preservation. The British Library, London 29-30 September. P197

Walters suggests that trust has to be built between organisations forming a co-operative group of institutions to undertake digital preservation, and compares this group of institutions to the Federal Reserve System in the USA which runs US central state bank. There are 12 Federal Reserve district banks which generate their own income, but all profits are returned to the central bank.

Holland examines virtual organizational models, and trust within them. He suggests that institutional trust is not institutional at all, and that trust is built between individuals working for institutions. He suggests that people in institutions grow trust between them, and then bring their institutions into partnership based on that trust. (11)

(11) Holland, C 1998. Proceedings of the Thirty-First Hawaii International Conference on System Sciences, v. 6: 602-10. P199



He further suggests that there must be a satisfactory level of assurance that each institution will perform their roles and responsibilities for the other. Trust is built organically and based upon the experiences each institution has with the other. Thus institutional trust, take on human qualities because it is established and maintained by people. It is both rational and emotional, as people are.

3.5 TRUST EQUATION

Maister posits the existence of a “trust equation”, which is expressed as; $\text{Credibility} + \text{Reliability} + \text{Intimacy} / \text{Self-Orientation} = \text{Trustworthiness}$

- 1) Credibility - comes from the mastery of our professional body of knowledge and how we communicate it.
- 2) Reliability - is about the actions taken to fulfil a promise or intention that was communicated. Creating opportunities to demonstrate reliability to prospective partners is best done “by making promises, explicit or implicit, and then delivering on them”
- 3) Intimacy – this refers to our emotional response to words and actions
- 4) Self interest – is about the sense of giving to others that permeates all collaborative work. (12)

(12) Maister, D et al “The trusted advisor” The Free Press; 2000

It therefore takes time and effort to develop trust relationships, as reliability can only be built up over time, as can self-orientation. It is therefore efficient to form preservation partnerships between institutions who have already invested in a trust relationship. This reduces costs, advancing the federation quickly, and with high-quality outcomes. Models for building them such as the trust equation helps us identify proper modes of conducting our “preservation business” inter-personally and inter-institutionally.

Breman also refers to Maister and the four components of trust, arguing that

“self-interest is weighted most heavily because the authors believe this is where the greatest risk for breaching trust lies” (13)

(13) Berman, Fran The Need to Formalize Trust Relationships in Digital Repositories EDUCAUSE Review, vol. 43, no. 3 (May/June 2008): 10–11

Berman has looked at the problems of digital preservation from the point of view of developing data grids to support digital repositories, and trust relationships within them. Such networks are used to host geographically distinct copies of digital objects in order to protect the data. Berman reports that general trust relationships among the collaborator institutions are formalised via Memoranda of Understanding, and service-oriented trust relationships are formalised via Service Level Agreements, as are many established information services. He suggests that the implementation of such structural mechanisms can be a means by which independent trust can be achieved.



4 QUESTIONNAIRE

4.1 INTRODUCTION

A questionnaire was constructed which aimed to explore attitudes in relation to trust within the digital preservation community, particularly those working on the CASPAR project. A copy of the questionnaire is included in Appendix 1.

The questionnaire was hosted online and invitations to answer it were circulated to three different groups:

- Group 1 were members of CASPAR testbeds
- Group 2 were members of discussion lists CASPAR testbeds members identified as relevant to the questionnaire
- Group 3 were members of further relevant email discussion lists.

Numbers of respondents were as follows

| Group 1 | Group 2 | Group 3 | total |
|---------|---------|---------|-------|
| 11 | 3 | 7 | 21 |

Although the numbers are small, it is felt that these results provide an important insight into the data holders in the CASPAR consortium, as initial representatives of the user community concerned with preservation.

4.2 RESPONDENTS

1) Subject area

There were 21 responses to the questionnaire, and the respondents defined themselves as working in the following areas

| | Group 1 | Group 2 | Group 3 | total | %age |
|-------------------|---------|---------|---------|-------|------|
| Performing arts | 5 | 0 | 1 | 6 | 29 |
| Cultural heritage | 1 | 0 | 4 | 5 | 24 |
| Science | 5 | 3 | 1 | 9 | 43 |
| | | | | | 96 |

(1 respondent did not answer this question.)

The questionnaire service used did not allow linked data to be analysed, so it is not possible to determine which responses came from which user community. It is therefore not possible to determine such things as whether all the respondents who work in performing arts are also curators of digital objects.

2) Job area

The posts held by those responding were either academic staff, managerial or technical as follows:

Group 1



Academic

- Department dean
- Professor
- Assistant Professor
- Research Fellow
- Director of Studies
- Manager pedagogy and research

Technical and managerial

- Head of Facilities Management
- Executive Director of a Foundation
- Remote sensing specialist
- Information Manager

Group 2

- Research fellow
- Senior EAI consultant

Group 3

- Product Manager
- Digital Services Librarian
- Open Collections Program Manager, University Library ; role = manage digitization projects and manage aggregated collections of digital objects
- Digital Data Repository Architect
- Musician
- University Archivist - care of university's own archives and also deposited archives used for research.

3) Roles in relation to digital objects

The roles of the respondents regarding digital objects were as follows:

| | | |
|---------------------------------|----|-----|
| Creator of digital objects | 6 | 30% |
| Curator of digital objects | 10 | 50% |
| User of curated digital objects | 4 | 20% |

Respondents were therefore mainly curators of digital objects, in senior academic or technical posts and working in science.

4.3 REPOSITORIES

This section largely asked questions about the importance of a factor in determining if a respondent trusts a repository. Responses were all on a scale of 0 -5, with 0 being “Not important” and 5 being “Very important”

Cumulative scores

Cumulative scores do not take into account the spread of scores, and are a crude measure. However, they do allow ranking of factors. These scores are sorted with highest score (most important) first for questions 4-15.



| | Question | Cumulative score |
|----|--|-------------------------|
| 7 | Track record of the repository's ability to curate objects | 83 |
| 10 | Repository conformity to international or national standards | 83 |
| 8 | The repository preserves the audit trail | 82 |
| 14 | Security of the contents of the repository | 82 |
| 9 | The control of integrity within the repository | 77 |
| 6 | Recommendation through professional network | 74 |
| 5 | Personal recommendation | 63 |
| 13 | Physical security of the repository building | 63 |
| 4 | Personal contact with staff at a repository | 62 |
| 11 | Repository has been validated by a toolkit DRAMBORA or TRAC | 45 |
| 12 | Repository has been validated by a domain-specific authority such as the Museums Documentation Association (MDA) | 40 |
| 15 | Marketing and passion | 39 |

Most important factors

There is a clear group here of the factors which are most important when determining whether to trust a repository. The four factors which score over 80 are

- Track record of the repository's ability to curate objects
- Repository conformity to international or national standards
- The repository preserves the audit trail
- Security of the contents of the repository

Significant factors

There is a further group of significant factors in deciding whether to trust a repository as follows:

- The control of integrity within the repository
- Recommendation through professional network
- Personal recommendation
- Physical security of the repository building
- Personal contact with staff at a repository

Least important factors

Similarly there are a group of factors which score under 60 which are clearly the least important when deciding on whether to trust a repository. The following three factors scores under 50

- Repository has been validated by a toolkit DRAMBORA or TRAC
- Repository has been validated by a domain-specific authority such as the Museums Documentation Association (MDA)
- Marketing and passion



16) The repository has well defined plans relating to its governance and operations.

Here an overwhelming majority of 82% responded 'yes' and 9% responded 'no'.

Those who indicated that plans in relation to governance were important were asked to indicate the importance of different types of plans, and the cumulative scores are below. Cumulative scores do not take into account the spread of scores, and are a crude measure. However, they do allow ranking of factors. These scores are sorted with highest score (most important) first

| | | Cumulative score |
|---|-------------------|-------------------------|
| E | Technical plan | 78 |
| I | Preservation plan | 76 |
| F | Data plan | 69 |
| D | Access plan | 66 |
| G | Succession plan | 65 |
| H | Disaster plan | 63 |
| B | Acquisition plan | 62 |
| C | Staffing plan | 61 |
| A | Business plan | 50 |

Most important factors

Two factors rank over 70 as follows

- Technical plan
- Preservation plan

Significant factors

The majority of factors are ranked as significant scoring between 61 and 69;

- Data plan
- Access plan
- Succession plan
- Disaster plan
- Acquisition plan
- Staffing plan

Least important

Business plan scored only 50 points, 11 points behind the second least important factor, and clearly the least significant type of plan for respondents. This is a very striking finding, as a repository without a firm business plan and therefore no guarantee of income is unlikely to survive, especially in the long term.

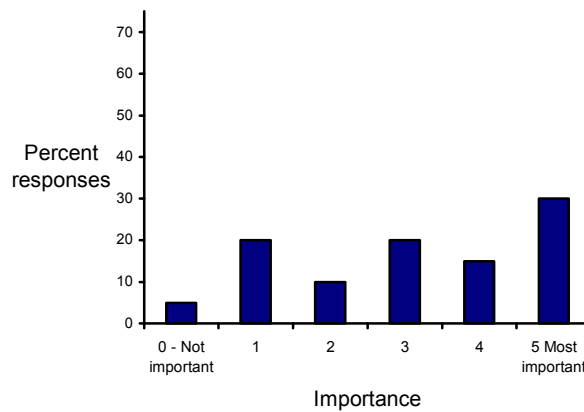


4.4 FULL QUESTIONNAIRE RESPONSES

Representing the full responses to the questionnaire and representing them graphically, allows the spread of responses to be examined. This is particularly useful for determining how much or little consensus there is between respondents. If there are responses for each of the scores as in Question 4 below, there is little consensus between the respondents. If there was full consensus between respondents, all responses would be for the same score, however this does not happen here. The closest the respondents get to consensus is with only 3 response scores being returned, so overall there is little consensus. Overall there is little consensus between respondents.

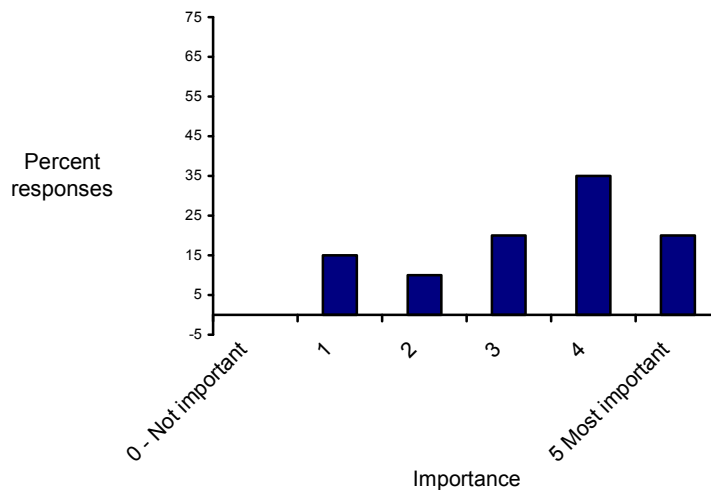
4) Personal contact with staff at a repository

There is a broad spread of scores here with responses for each of the six possible scores. This indicates a lack of consensus amongst respondents, although the majority are on the ‘most important’ side of the scale.



5) Personal recommendation (a colleague tells you about it)

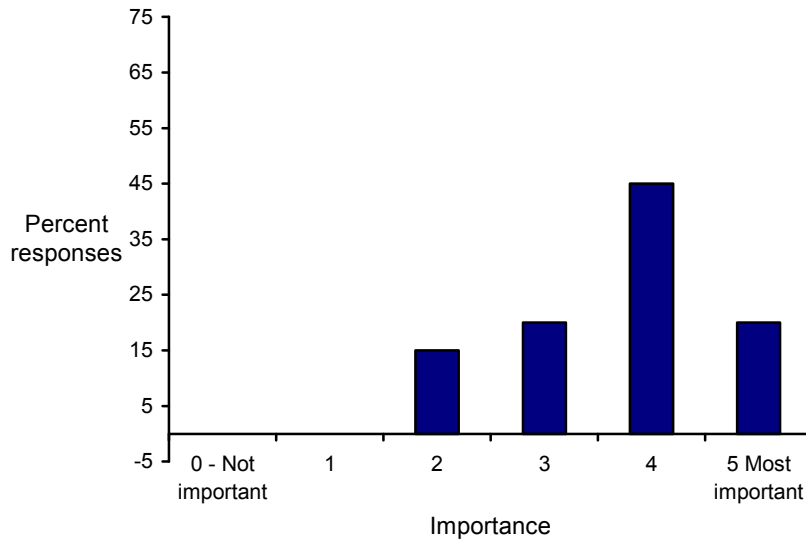
There is a significant spread of scores here again with responses for 5 of the six possible scores, and this indicates a lack of consensus amongst respondents. Again the majority of scores are on the ‘most important’ side of the scale.





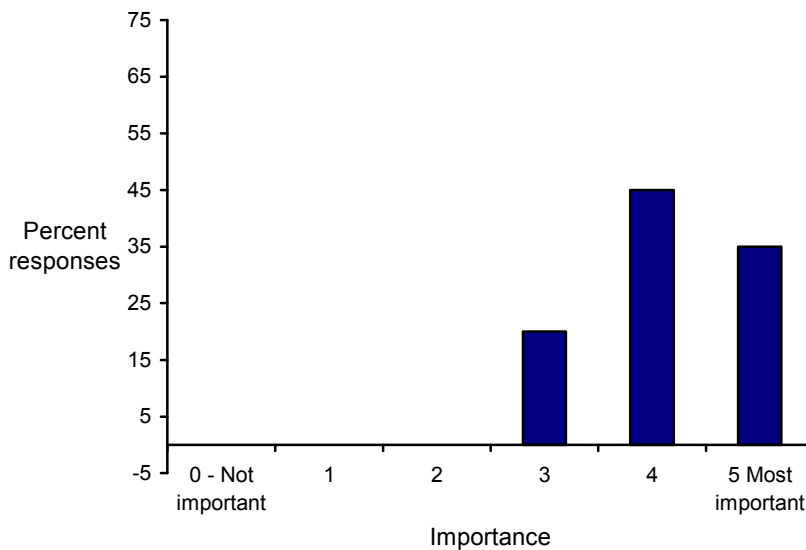
6) Recommendation through professional network (email discussion lists, conferences and seminars, journal/magazine articles)

A tighter spread of responses here with responses for 4 of the possible 6 scores. There are no responses for ‘0’ Not important’ or ‘1’, and the majority of responses are for ‘4’.



7) Track record of the repository’s ability to curate objects and to provide reliable efficient access to authentic objects over time (examples of the repositories’ previous work)

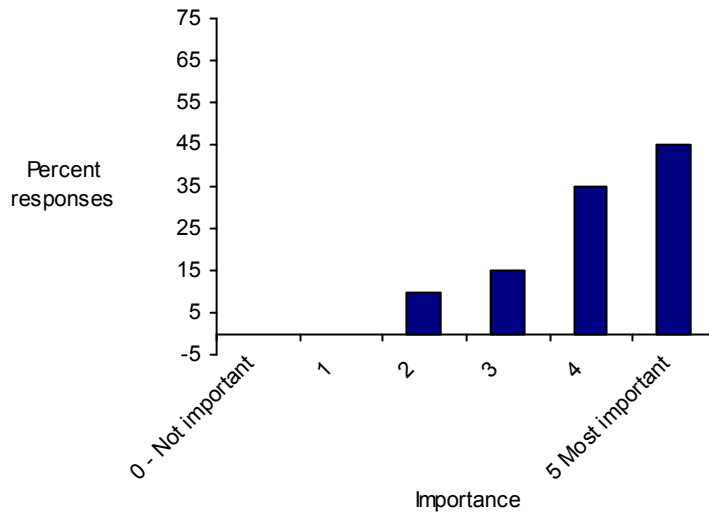
A small spread of responses here indicating consensus amongst respondents, with responses for only 3 of the 6 possible scores. There are no responses for ‘0’ Not important’, or for scores of ‘1’ or ‘2’, and the majority of responses are for ‘4’.





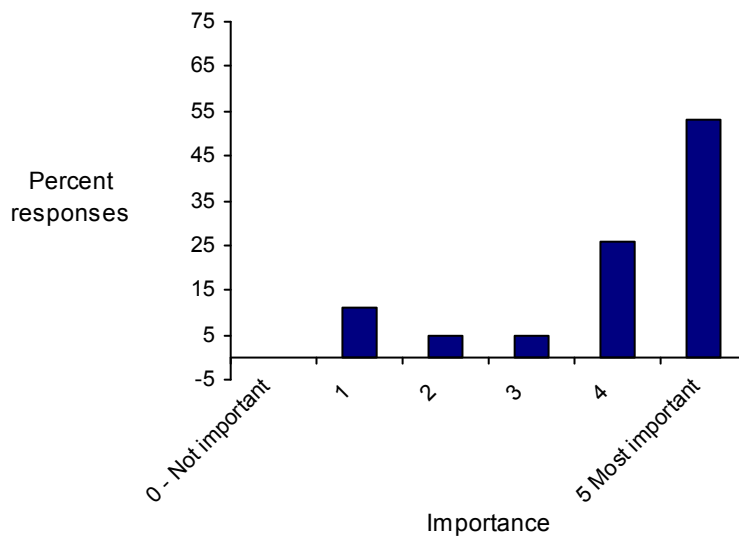
8) The repository preserves the audit trail and documents the preservation processes. The repository can demonstrate reliable and efficient access to authentic objects over time.

A spread of responses here with responses for 4 of the possible 6 scores. There are no responses for ‘0’ Not important’ or for ‘1’, and the majority of responses are for ‘5 Most important’.



9) The control of integrity within the repository (e.g. digest, checksum, digital signature, other)

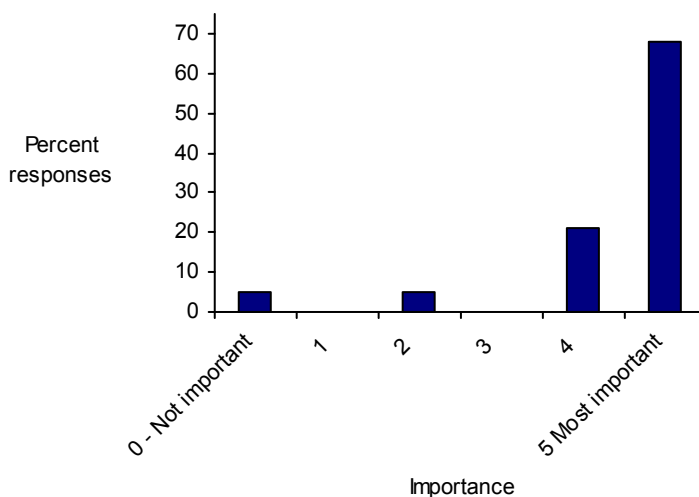
A spread of responses here with responses for five out of six categories, showing a lack of consensus. However, the clear majority of respondents giving a score of ‘5 Most important’.





10) Repository conformity to international or national standards

There was a broad spread of responses here with 5% giving a responses of '0 Not important', and no responses for scores of '1' or '3'. A significant majority of 65% give a score of '5 Most important'.



Those respondents who replied that standards were important were asked to indicate which standards from a list, and could select as many standards as they wished. The standards listed below have been sorted by number of responses.

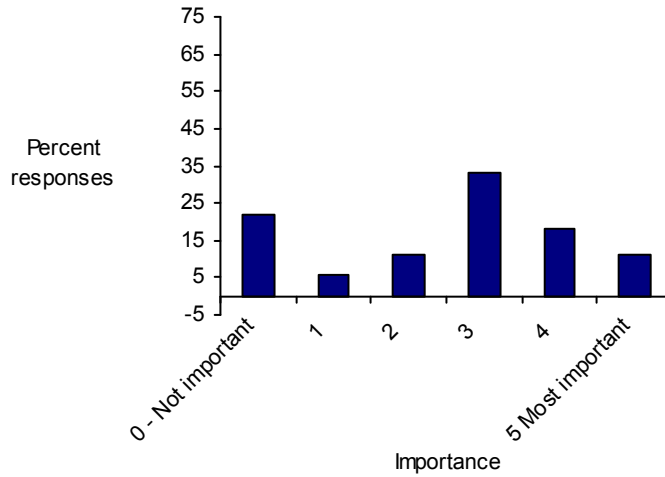
| | |
|--|---|
| ISO 23081-1:2006 Information and documentation -- Records management processes -- Metadata for records | 8 |
| ISO 9001:2000 Quality management systems | 7 |
| ISO 15489-1:2001 Information and documentation. Records management. General | 7 |
| ISO11799 : 2003 Information and documentation - Storage requirements for archive and library materials | 7 |
| Others | 6 |
| ISO/IEC 17799:2005 Information technology. Security techniques. Code of practice for information security management | 4 |
| ISO/IEC 27001:2005 Information technology. Security techniques. Information security management systems | 4 |
| sector standards CIDOC/CRM (international museums) | 2 |
| sector standards Spectrum (UK museum) | 1 |

Four standards were indicated by 7 or 8 respondents; two records management standards, one quality standard and one storage standard. Four other standards were indicated by less than 5 respondents, and these were two IT security standards and sector standards.

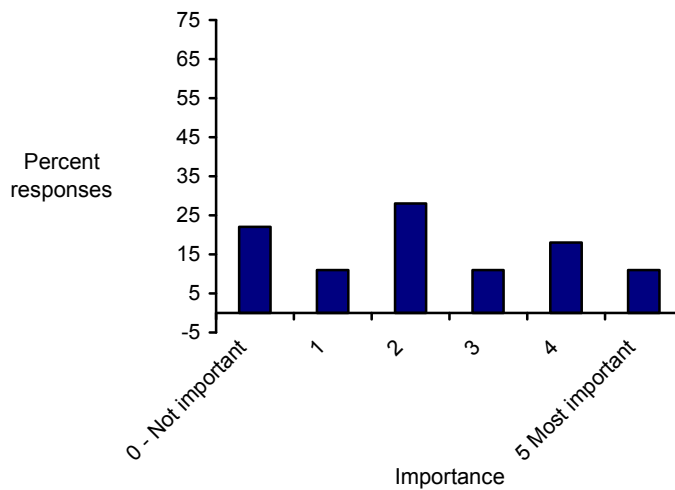


11) Repository has been validated by a toolkit such as Digital Repository Audit Based on Risk Assessment (DRAMBORA), or Trusted Repositories Audit Criteria (TRAC) Please indicate the level of importance where 0 is not important and 5 is very important

There was a broad range of response here, indicating a lack of consensus amongst respondents.



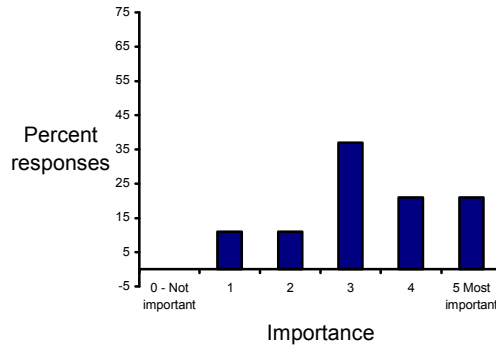
12) Repository has been validated by a domain-specific authority such as the Museums Documentation Association (MDA)





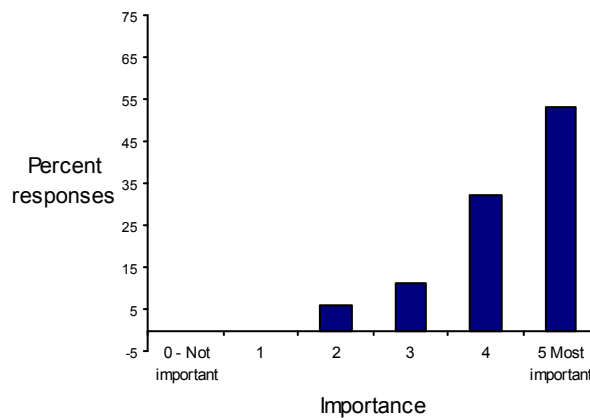
13) Physical security of the repository building

Here there were an equal number of respondents (27%) giving a response of 5 and of 3, with 18% giving a score of 4 and 2. This shows a considerable spread between medium and most important.

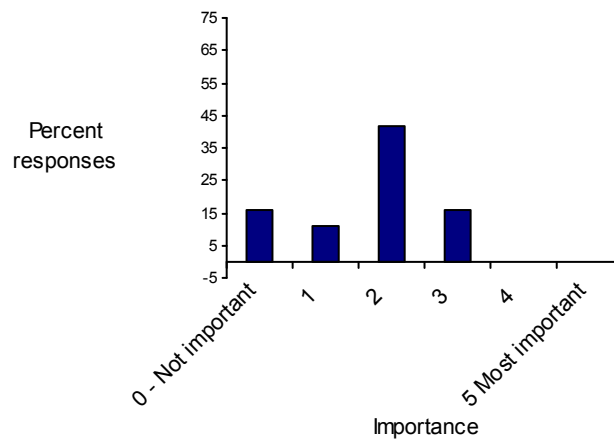


14) Security of the contents of the repository (e.g. the objects are secured against corruption – either intentional or unintentional)

Here the majority of respondents (36%) gave a response of 5 out of 5.



15) Marketing and passion

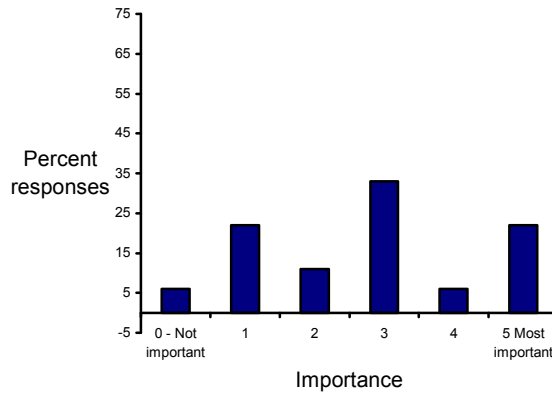




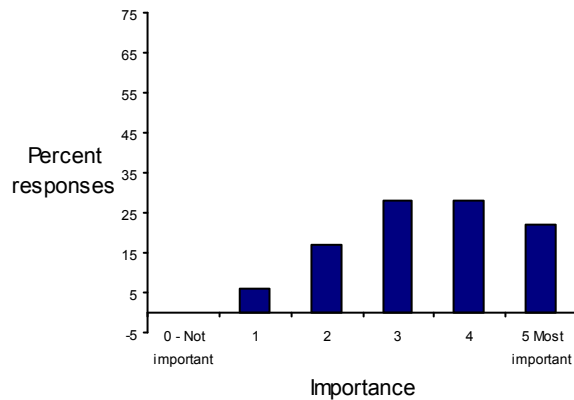
16) The repository has well defined plans relating to its governance and operations.

Here 89% responded ‘yes’ and 11% responded ‘no’. Those who indicated that plans in relation to governance were important were asked to indicate the importance of different types of plans, and responded as follows:

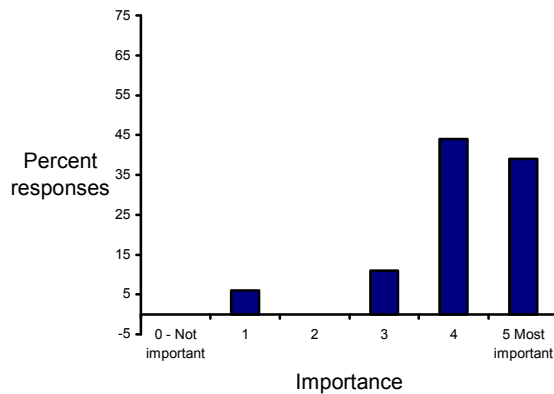
a) Business plan



b) Acquisition plan

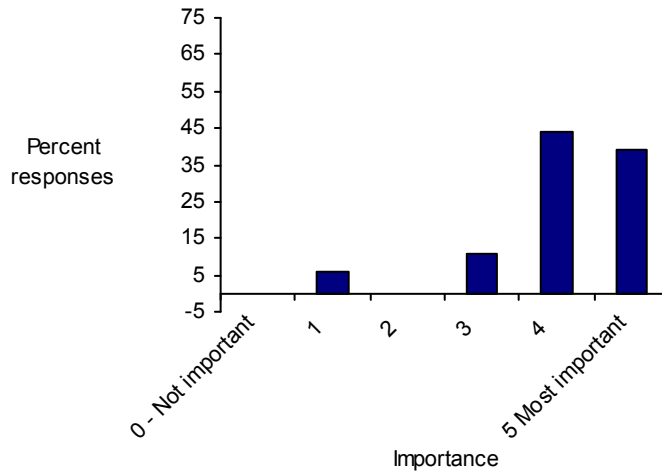


c) Staffing plan

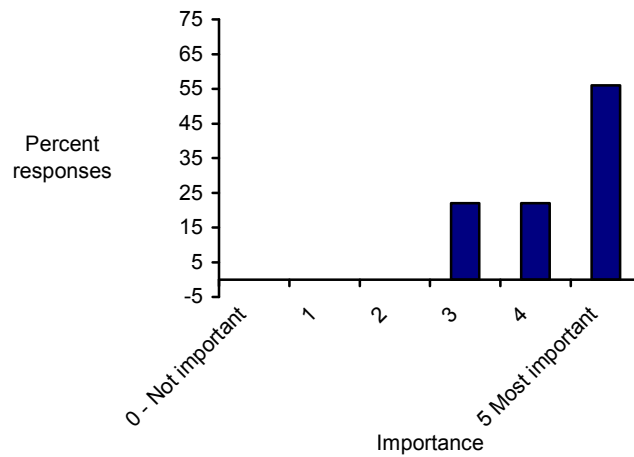




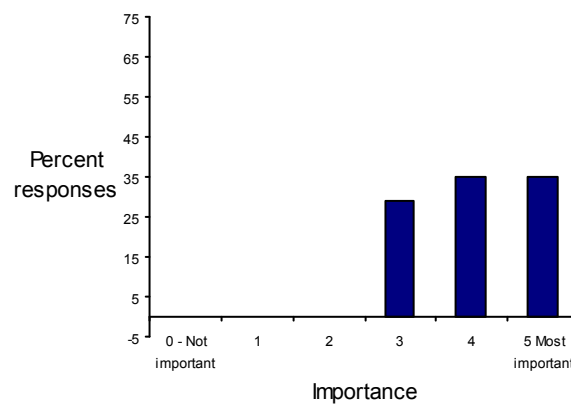
d) Access plan



e) Technical plan

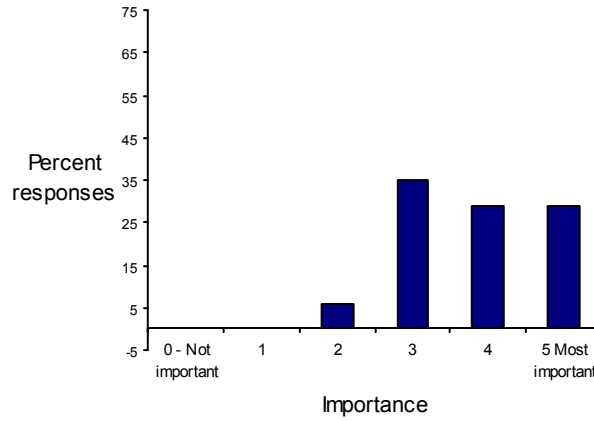


f) Data plan

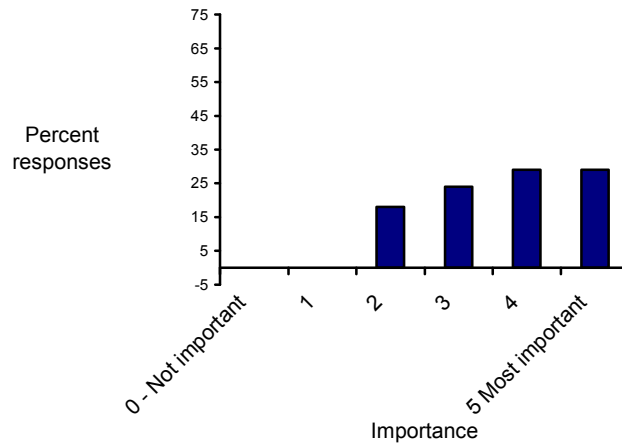




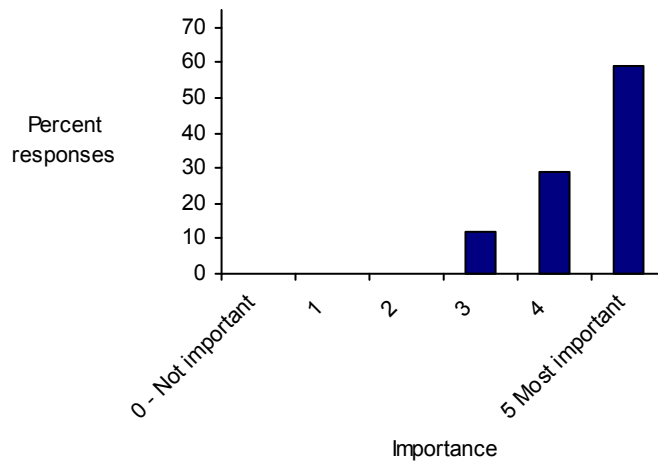
g) Succession plan (for after the repository ceases to exist)



h) Disaster plan



i) Preservation plan





17) Are there any other elements which help you decide if a repository is trustworthy? If so please describe them below.

‘This survey does not apply since I am still finding out what is the real ideal way of preserving digital material. All tests until present have failed. I am still keeping old tapes and LPs in my repository being curious if my new method of keeping the recordings on a hard disk in wav. format is a "solution". The DAT system failed The CD system failed The DVD system failed The audio data failed I am exploring flac,mp3 and wav. 16 bit on hard disk. In 5 years we will find out results. The other questions you put up in your survey are rubbish to me. Sorry for being so drastic and critical. The sound industry has no interest in helping out, they still do not publish how they store their original. SONY should be the right interlocutor, they own Film Industry repositories (MGM), sound repositories (Columbia) , produce sound equipment and sound supports (CD,DVD,DAT,etc.) They want to make business in the future with their repositories.’

‘Assessment by various users and operators to define what is better to be preserved (i.e. reduce to the minimum the unnecessary duplication)’

Other responses

There were some responses emailed directly, rather than being left as comments on the survey as follows

1) ‘Thank you for asking me participate in your survey. I would like to help, since I also participate in other European projects and I have colleagues at IRCAM. So, I started to fill the questionnaire. Unfortunately I do not understand many of the questions (for example: curation?, curate objects?), so I can't really answer them. Probably then I am not the kind of person that you would like to include in your study. I hope that you will find other persons who understand better and actually work with digital repositories. Good luck with your research.’

2) ‘I am sorry to not have responded, I looked at it and I really cannot respond most of the questions. So I will not do it, sorry’.

3) ‘I looked at your questionnaire and felt that I was out of my depth with the more archive-specific questions. Perhaps you should discuss this with the repository initiatives’

4) ‘the questions in this questionnaire do not seem to apply to me at all.’



4.5 CONCLUSIONS FROM THE SURVEY

Respondents to the questionnaire were mainly curators of digital objects, in senior academic or technical posts and working in science. There was little consensus between respondents, indicated by a wide spread of responses.

Factors in determining trust

There were four factors with cumulative scores of over 80 in determining if a respondent trusts a repository, as follows:

- Track record of the repository's ability to curate objects
- Repository conformity to international or national standards
- The repository preserves the audit trail
- Security of the contents of the repository

There were three factors with cumulative scores below 40 as follows:

- Repository has been validated by a toolkit DRAMBORA or TRAC
- Repository has been validated by a domain-specific authority such as the Museums Documentation Association (MDA)
- Marketing and passion

Evidence of previous effective curation and conformity to international standards are therefore the most important factors in determining whether to trust a repository, as expected. Good intentions and conformance to domain specific standards and toolkits were the least important.

Importance of planning

Two types of plan were identified as most important in relation to governance and operations, with cumulative scores of over 70

- Technical plan
- Preservation plan

One factor was found to be least important with a cumulative score of under 50 of Business plan. This is somewhat surprising, as most of the respondents are senior management, but rate a business plan as least important of all the plans. Without an effective business plan a repository could run into financial and management difficulties, and may not be able to maintain its holdings. A good technical plan and preservation plan are no good, if there is not the finance and personnel to carry them out.



5 STANDARDS

5.1 INTRODUCTION

In a comparatively new area such as digital preservation, it can be difficult to find national and international standard to conform to in order to try and engender trust. However, there may be established standards from other domains which may be relevant and could be applied. In the area of digital preservation, overall assurances of the quality of work undertaken by an OAIS could be given if it was audited and certified to be in conformance with ISO 9001 Quality Management Systems. Further key standards which could be applied to a digital repository are ISO 27001 Information Technology Security techniques and management Systems, and ISO 17799 Information technology – security techniques.

More specific audit and certification procedures have been developed which are specific to the digital preservation environment and aim to provide quality assurance for repository users, and provide objective evidence that repositories are conforming to a set of standards. Various organisations have undertaken work in this area including DCC and DPE, RLG and OCLC, OCLC and CRL and nestor. Aspects of a repository to which audit and certification practice can be applied include the organisational framework, object management, infrastructure and security. Specific areas which may be audited include: definition of goals, usage and access, observation of legal and contractual rules, appropriateness of levels of finance and staffing, long term strategic planning and quality management planning.

5.2 OVERVIEW OF RELEVANT ISO STANDARDS

BS ISO/IEC 27002:2005, BS 7799-1:2005, BS ISO/IEC 17799:2005

Information technology. Security techniques. Code of practice for information security management

This standard is the UK implementation of ISO 27002: 2005 and it supersedes ISO 17799:2000, which is withdrawn.

This standard established guidelines and general principles for initiating, implementing maintaining and improving information security management in organisations. The objectives outlined provide general guidance on the commonly accepted goals of information management security.

The control objectives and controls of this standard are intended to be implemented to meet the requirements identified by a risk assessment. The standard may serve as a practical guideline for developing organisational security standards and effective security management practices and to help build confidence in inter-organisational activities.

BS ISO/IEC 27001:2005

Information technology. Security techniques. Information security management systems. Requirements.

BS ISO/IEC 27001:2005 covers all types of organisations (e.g. commercial enterprises, government agencies, non-profit organisations) and specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system (ISMS) within the context of the organisation's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organisations.

The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. If an



organisation already has an operative business process management system (e.g. in relation to ISO 9001 or ISO 14001), it is preferable in most cases to satisfy the requirements of this International Standard within the existing management system.

BS EN ISO 9000:2005 Quality management systems.

Fundamentals and vocabulary

BS EN ISO 9000:2005 supersedes BS EN ISO 9000:2000 which is withdrawn.

The BS EN ISO 9000 family of standards is primarily concerned with “quality management”. Everyone may have a slightly different idea as to what “quality” is, but in the standard the definition refers to all those features of a product (or service) which are required by the customer.

“Quality Management” means what the organisation does to ensure that its products or services satisfy the customer's quality requirements and comply with any regulations applicable to those products or services.

Used together the standards form a coherent quality management system (QMS), although they can also be used independently.

BS EN ISO 9000:2005 describes fundamentals of a QMS, which form the subject of the BS EN ISO 9000 family, and defines related terms.

Abstract

This International Standard describes the fundamentals of quality management systems, which form the subject of the ISO 9000 family of standards, and defines related terms.

This International Standard is applicable to the following:

- a) Organisations seeking advantage through the implementation of a quality management system
- b) Organisations seeking confidence from their suppliers that their product requirements will be satisfied
- c) users of the products
- d) those concerned with a mutual understanding of the terminology used in quality management (e.g. suppliers, customers, regulators)
- e) Those internal or external to the organisation who assess the quality management system or audit it for conformity to the requirements of ISO 9001 (e.g. auditors, regulators, certification/registration bodies)
- f) Those internal or external to the organisation who give advice or training on the quality management system appropriate to that organisation
- g) developers of related standards.

BS EN ISO 9000-1:1994

Quality management and quality assurance standards. Guidelines for selection and use

Clarifies the principal quality concepts and provides guidance on the selection and use of the ISO 9000 family of standards on quality systems that can be used for internal quality management purposes and for external quality assurance purposes.

BS ISO 9000-2:1997



Quality management and quality assurance standards. Part 2 - generic guidelines for the application of ISO 9001, ISO 9002 and ISO 9003

This part of ISO 9000 gives guidance for the application of ISO 9001, and ISO 9002 and ISO 9003 which are both withdrawn.

BS EN ISO 9001:2000 Quality management systems. Requirements

BS EN ISO 9001:2000 specifies requirements for a QMS where an organisation: needs to demonstrate its ability to consistently provide product that meets customer and applicable regulatory requirements, and aims to enhance customer satisfaction through the effective application of the system. This includes processes for continual improvement of the system and the assurance of conformity and applicable regulatory requirements.

One of the fundamental purposes of BS EN ISO 9001:2000 is to enable the development of a QMS that is fully integrated into the normal operations of your business. This standard avoids the application of systems that are separate from your organisation's business processes. Therefore, it creates a more logical and effective approach to managing an organisation which is process-based.

5.3 OTHER RELEVANT STANDARDS

PD 0018:2001 Information management systems. Building systems fit for audit

Hardcopy Only ISBN0 580 33267 5

Descriptors Quality auditing, Management, Information, Documents, Records (documents), Records management, Information handling, Data processing, Data security, Quality assurance systems, Risk assessment, Verification IT and Information Management: IT Service Management.

BS ISO/IEC 15910:1999 Information technology. Software user documentation process

This standards main activity is the creation of a comprehensive plan for developing documentation, as the ever increasing complexity of software makes necessary the availability of complete, accurate and understandable documentation to those who use the software.

BS ISO 20652:2006

Space data and information transfer systems. Producer-archive interface.

This international standard identifies, defines and provides structure to the relationship and interaction between an information producer and archive. It defines the methodology for the structures of actions that are requires from the initial time of contact between the producer and the archive until the objects of information are received and validated by the archive. These actions cover the first stages of ingest process as defined in the open archival information system (OASI) reference model. This standard describes parts of the functional entities administration and ingest.

BS 5454:2000

Recommendations for the storage and exhibition of archival documents.

These recommendations apply to the long-term, permanent storage of archival documents. The temporary storage of such documents in restricted access and their



display in exhibitions is also covered. The recommendations apply to new buildings, whether purpose-built or adapted, and to existing buildings.

The recommendations in BS 5454:2000 mainly concern traditional materials, i.e. paper and parchment, although some guidance on more modern media is given in clause 11. This guidance is intended for the storage of modern media in general-purpose repositories, and further specialist advice may also be required.

BS 5454:2000 is for use by those concerned with the planning, construction, equipment, maintenance and working of such repositories.

BS ISO 21127:2006

Information and documentation. A reference ontology for the interchange of cultural heritage information

- This standard is the culmination of more than a decade of standards development work by the International Committee for Documentation (CIDOC) of the International Council of Museums (ICOM). Throughout its development the model has been known as the 'CIDOC Conceptual Reference Model' or CRM.
- The primary purpose of this International Standard is to offer a conceptual basis for the mediation of information between cultural heritage organisations such as museums, libraries and archives. The standard aims to provide a common reference point against which divergent and incompatible sources of information can be compared and ultimately harmonised.

BS ISO 23081-1:2006 Information and documentation. Records management processes. Metadata for records. Principles

This standard addresses the relevance of records management metadata in business processes, as well as the different roles and types of metadata that support business and records management processes. It also sets a framework for managing these metadata.

DD ISO/TS 23081-2:2007 Information and documentation. Records management processes. Metadata for records. Conceptual and implementation issues

This technical specification establishes a framework for defining metadata elements consistent with the principles and implementation considerations outlined in ISO 23081-1:2006. The purpose of the framework is to

- Enable standardised description of records and critical contextual entities for records.
- Provide common understanding of fixed points of aggregation to enable interoperability of records, and information relevant to records, between organisational systems.
- Enable reuse and standardisation of metadata for managing records over time, space and across applications.

MLA The Accreditation Scheme for Museums in the United Kingdom: Accreditation Standard

This accreditation scheme sets nationally agreed standards for UK museums. To quality museums must meet clear basic requirements on how they care for and document their collections, how they are governed and managed, and on the information and services they offer to their users. Accreditation benefits museum visitors and the users of museum services. It supports museum managers and governing bodies in planning and



developing their services, and it provides a benchmark for grant-making organisations and donors.

Capability Maturity Model Integration

Capability Maturity Model[®] Integration (CMMI) is a process improvement approach that provides organisations with the essential elements of effective processes. It can be used to guide process improvement across a project, a division, or an entire organisation. CMMI helps integrate traditionally separate organisational functions, set process improvement goals and priorities, provide guidance for quality processes, and provide a point of reference for appraising current processes.

There is a comprehensive list of standards relevant to digital preservation DCC DIFFUSE Standards Registry at <http://www.dcc.ac.uk/diffuse/>



6 STANDARD AND CERTIFICATION

Put at its simplest, a standard is an agreed, repeatable way of doing something. It is a published document that contains a technical specification or other precise criteria designed to be used consistently as a rule, guideline, or definition. Standards help to make life simpler and to increase the reliability and the effectiveness of many goods and services. They are intended to be aspirational - a summary of good and best practice rather than general practice. Standards are created by bringing together the experience and expertise of all interested parties such as the producers, sellers, buyers, users and regulators of a particular material, product, process or service.

Any standard is a collective work. Committees of manufacturers, users, research organisations, government departments and consumers work together to draw up standards that evolve to meet the demands of society and technology.

ISO standards are developed according to the following principles.

- Consensus.
The views of all interests are taken into account: manufacturers, vendors and users, consumer groups, testing laboratories, governments, engineering professions and research organisations.
- Industry wide.
Global solutions to satisfy industries and customers worldwide.
- Voluntary.
International standardization is market driven and therefore based on voluntary involvement of all interests in the market-place.

There are three main phases in the ISO standards development process as follows.

1. The need for a standard is usually expressed by an industry sector, which communicates this need to a national member body. The latter proposes the new work item to ISO as a whole. Once the need for an International Standard has been recognised and formally agreed, the first phase involves definition of the technical scope of the future standard. This phase is usually carried out in working groups which comprise technical experts from countries interested in the subject matter.
2. Once agreement has been reached on which technical aspects are to be covered in the standard, a second phase is entered during which countries negotiate the detailed specifications within the standard. This is the consensus-building phase.
3. The final phase comprises the formal approval of the resulting draft International Standard (the acceptance criteria stipulate approval by two-thirds of the ISO members that have participated actively in the standards development process, and approval by 75% of all members that vote), following which the agreed text is published as an ISO International Standard.

There are variants of these phases and OAIS demonstrates one of these. OAIS development was hosted by the Consultative Committee for Space Data Systems (see <http://www.ccsds.org>) which is effectively the working arm of TC20/SC13. The standards are approved by CCSDS and then go through the ISO formal approval process. This process is being adopted by the Repository Audit and Certification Working Group (RAC – see <http://wiki.digitalrepositoryauditandcertification.org>). RAC is developing two related standards:

- Metrics for Digital Repository Audit and Certification- using new template for metrics
- Requirements for Bodies Providing Audit and Certification of Digital Repositories



6.1 TYPES OF ACCREDITATION

There are two types of accreditation, those undertaken by an organisation internally and those undertaken by external accreditation bodies. The ISO 9000 family of quality standards may be administered either externally or internally. Accreditation administered by an external body is generally perceived to be more rigorous than one administered internally.

An example of an external accreditation body is the MLA who administers Accreditation Scheme for Museums in the United Kingdom. Museums Libraries Archives Council is Non-Departmental Public Body (NDPB), which is sponsored by the Department for Culture, Media and Sport (DCMS). As the DCMS also funds the Library Archives and Museums, there is some pressure on institutions to become accredited.

For a certification process the following is needed

- a set of procedures that cover all key processes in the business
- monitoring processes to ensure they are effective
- adequate record keeping
- checking output for defects, with appropriate corrective action where necessary
- regularly reviewing individual processes and the quality system itself for effectiveness
- facilitating continual improvement

6.2 HOW ARE ACCREDITATION BODIES SET UP?

There is an international standard for certification bodies, “**ISO 17021: 2006 Conformity assessment – requirements for bodies providing audit and certification of management systems**”. If an accreditation system were to be established for digital preservation repositories which is implemented by an external body, then it should comply with this standard.

As digital preservation is essentially a management process ISO 17021 is an appropriate standard to apply to a body providing certification for repositories. The standard contains principles and requirements for the competence, consistency and impartiality of the audit and certification of management systems of all types and for bodies providing these activities. Certification of management systems is a third-party conformity assessment activity, and bodies performing this activity are therefore third-party assessment bodies.

For example RAC is developing the *Requirements for Bodies Providing Audit and Certification of Digital Repositories* which is conformant with ISO 17021.

The overall aim of certification is to give confidence to all parties that a management systems fulfils specified requirements, and the value of certification is the degree of public confidence and trust that is established by an impartial and competent assessment by a third party. Parties that have an interest in certification include: the clients of the certification body, the customers of the organisations whose management systems are certified, governmental authorities, non-governmental authorities and consumers and members of the public.

The **United Kingdom Accreditation Service** is a non-profit-distributing company, limited by guarantee, which operates through a memorandum of understanding with the government through the Secretary of State for Innovation, Universities and Skills. UKAS is the sole national accreditation body recognised by Government to assess organisations that provide certification testing inspection and calibration services, against internationally agreed standards.

http://www.ukas.com/about_accreditation/default.asp

European Network for Accreditation is a non-profit association set up in November 1997 and registered as an association in the Netherlands in June 2000. EA is a European network of nationally recognised accreditation bodies based in the European geographical area.

<http://www.european-accreditation.org/content/ea/EuropNetwork.htm>



7 CONCLUSIONS

The survey results, albeit with poor statistical significance, show that evidence of previous effective curation and conformity to international standards are the most important factors in determining whether to trust a repository; good intentions and conformance to domain specific standards and toolkits were the least important.

These conclusions are not unexpected but will be checked by wider and more detailed consultations in collaboration with the PARSE.Insight and DCC projects.

The route by which RAC is proposing to set up an accreditation, audit and certification process for digital repositories seems to be consistent with the findings of this report.



8 REFERENCES

CRL,(2007), Retrieved from <http://www.crl.edu/content.asp?l1=13&l2=58&l3=162&l4=92>

Dale, R., (2007), Mapping of Audit & Certification Criteria for CRL Meeting (15-16 January 2007). Retrieved from http://wiki.digitalrepositoryauditandcertification.org/pub/Main/ReferenceInputDocuments/TRAC-Nestor-DCC-criteria_mapping.doc

Garrett, J. & Waters, D, (Eds). (1996). Preserving Digital Information, Report of the Task Force on Archiving of Digital Information commissioned by The Commission on Preservation and Access and The Research Libraries Group. Retrieved from <http://www.ifla.org/documents/libraries/net/tfadi-fr.pdf>

Giaretta, D., (2008), Comparison of OAIS and the Chicago Meeting 10 points. Retrieved from <http://wiki.digitalrepositoryauditandcertification.org/bin/view/Main/ComparisonOaisAndChicago10Points>

nestor Working Group Trusted Repositories – Certification, (2006), Catalogue of Criteria for Trusted Digital Repositories. English version retrieved from <http://edoc.hu-berlin.de/series/nestor-materialien/8en/PDF/8en.pdf>

National Science Foundation Cyberinfrastructure Council (NSF, 2007), Cyberinfrastructure Vision for 21st Century Discovery. Retrieved from <http://www.nsf.gov/pubs/2007/nsf0728/nsf0728.pdf>

Open Archival Information System (OAIS) – Reference Model, ISO 14721:2003, (2003). Retrieved from <http://public.ccsds.org/publications/archive/650x0b1.pdf>

RLG-OCLC, (2002), Report on Trusted Digital Repositories: Attributes and Responsibilities. Retrieved from <http://www.oclc.org/programs/ourwork/past/trustedrep/repositories.pdf>

Ross, S., Bütikofer, N., and McHugh, A. (2006), DCC Comments on RLG/NARA Audit and Certification Checklist. Retrieved from http://wiki.digitalrepositoryauditandcertification.org/pub/Main/ReferenceInputDocuments/Ross_McHugh_Buetikofer_comments_RLGNARA_AUDIT_ver2.pdf

TRAC, (2007), Trustworthy Repositories Audit & Certification: Criteria and Checklist. Retrieved from <http://www.crl.edu/PDF/trac.pdf>



9 BIBLIOGRAPHY

1. Anon. BS EN ISO 9000-1: 1994 Quality management and quality assurance standards - Part 1: Guidelines for selection and use. 1-28. 1-7-1994. British Standards Institute.
Ref Type: Generic
2. Anon. BS ISO 9000-2: 1997 Quality management and quality assurance standards - Part 2: Generic guidelines for the application of ISO 9001, ISO 9002 and ISO 9003. 15-8-1997. British Standards Institute.
Ref Type: Generic
3. Anon. BS 5454:2000 Recommendations for the storage and exhibition of archival documents. 1-30. 2000. British Standards Institute.
Ref Type: Generic
4. Anon. The accreditation scheme for museums in the United Kingdom: accreditation standard. 1-60. 2004. Birmingham, Museum Libraries and Archives Council (MLA).
Ref Type: Generic
Abstract: MLA's Accreditation Scheme sets nationally agreed standards for UK museums. To qualify, museums must meet clear basic requirements on how they care for and document their collections, how they are governed and managed, and on the information and services they offer to their users. Accreditation benefits museum visitors and the users of museums services. It supports museum managers and governing bodies in planning and developing their services, and it provides a benchmark for grant-making organisations, sponsors and donors.
5. Anon. BS ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management. 1-130. 15-6-2005. British Standards Institute.
Ref Type: Generic
6. Anon. BS ISO/IEC 17799: 2005 BS 7799-1: 2005 Information technology - security techniques - code of practice for information security. 1-130. 16-6-2005. British Standards Institute.
Ref Type: Generic
7. Anon. BS ISO/IEC 27001:2005 Information technology - security techniques - information security management systems - requirements. 1-44. 18-10-2005. British Standards Institute.
Ref Type: Generic
8. Anon. BS ISO 20652:2006 Space data and information transfer systems - producer-archive interface - methodology abstract standard. 1-86. 16-3-2006. British Standards Institute.
Ref Type: Generic
9. Anon. BS ISO 21127:2006 Information and documentation - a reference ontology for the interchange of cultural heritage information. 1-118. 31-10-2006. British Standards Institute.
Ref Type: Generic



10. Anon. BS EN ISO 9000: 2005 Quality management systems - fundamentals and vocabulary. 1-42. 2008. British Standards Institute.
Ref Type: Generic
11. Anon. BS EN 17021: 2006 Conformity assessment - requirements for bodies providing audit and certification of management systems. 1-38. 2008. British Standards Institute.
Ref Type: Generic
12. Bachman R, Zaheer A. Handbook of trust research. Cheltenham: Edward Elgar Publishing; 2006.
13. Berman F, Kozbial A, McDonal, Robert H. The need to formalize trust relationships in digital repositories. *EDUCAUSE Review* 2008;43(3):10-1.
14. Bradley R. Digital authenticity and integrity: digital cultural heritage documents as research resources. *Portal: Libraries and the Academy* 2005;5(2):165-75.
15. Burmester M, Mulholland J. The advent of trusted computing: implications for digital forensics. 2006.
Abstract: The release of computer hardware devices based on "trusted computing" technologies is heralding a paradigm shift that will have profound implications for digital forensics. In this paper, we map out the contours of a trusted environment in order to establish the context for the paper. This is followed by the main components of the TC architecture with an emphasis on the Trusted Platform and the Trusted Platform Module (TPM). The next section presents a synopsis based on three threat models, viz., (i) pc owner-centric, (ii) trusted computing-centric, and (iii) digital forensics-centric and then briefly touches on the implications and unintended consequences of trusted computing for digital forensics. Finally, the last section of the concludes with a recommendation on how to mitigate the negative effects of trusted computing.
Notes: ISBN 1595931082
16. Candela, A, Castelli, A, Ioannidis, Y, and et al. The DELOS digital library reference model foundations for digital libraries version 0.96 . 2007. DELOS Network of Excellence on Digital Libraries.
Ref Type: Report
17. Cheung CMK, Lee MKO. Understanding consumer trust in Internet shopping: A multidisciplinary approach. *Journal of the American Society for Information Science and Technology* 2007;57(4):497-2.
18. Dobratz, Susanne and et al. Catalogue of criteria for trusted digital repositories: version 1. 1-48. 2006. Frankfurt am Main, nestor working group: trusted repositories - certification.
Ref Type: Report
19. Dobratz S, Schoger A, Strathmann S. The nestor catalogue of criteria for trusted digital repository evaluation and certification. 2006.
20. Dobratz S, Schoger A. Trustworthy digital long-term repositories: the nestor approach in the context of international developments. Berlin: Springer-Verlag; 2007.
21. Duranti L. Reliability and authenticity: the concepts and their implications. *Archivaria* 1995;39:5-10.



22. Dutton WH, Shepherd A. Trust in the Internet as an experience technology. *Information, Communication & Society* 2006;9(4):433-51.
Abstract: Trust in the Internet and related information and communication technologies - 'cybertrust' - could be critical to the successful development of 'e-services', such as e-government, e-commerce, e-learning and democratic participation in the rapidly expanding online public sphere. This paper explores trust in cyberspace based on an analysis of data from an Oxford Internet Survey conducted by the Oxford Internet Institute using a multi-stage, national probability sample in Great Britain. The paper highlights various perspectives on the meaning of trust and draws on findings from the Oxford Internet Survey to explore and refine key social determinants of cybertrust. Evidence from this research provides fresh insights into the factors shaping trust in the Internet, arguing that cybertrust, defined as a confident expectation, is influenced by experience, defined operationally by several indicators of proximity to the Internet, in ways shaped by educational background. The potential for using these results to better understand the role of trust on Internet use is addressed, as well as the more indirect implications for reinforcing digital divides.
23. Eastwood T. How goes it with appraisal? *Archivaria* 2003;93(111):121.
Abstract: Edited version of a keynote address given at the annual conference of the Associations of Canadian Archivists in Banff, Alberta, 22 May 91. Understanding the properties of archives and the processes forming them is important in the exercise of appraisal. Considers the capacities of archives, the nature of the act of projecting continuing value, and the part that knowledge of the properties and processes of any given archives plays in the art of appraisal. Examines the 3 recognized dimensions of value as grounds for appraisal: provenance of the documents; pertinence of the documents; and use, or value for survival and continuity of the society that created them. Emphasizes the need for professional objectivity, to understand the whole of interrelated documents comprising any given archives, and to refine methods of assembling and analysing the evidence on which archivists projections are based.
24. Francis L.Jeffries. Subjective norms, dispositional trust, and initial trust development. *Journal of Behavioral and Applied Management* 2002;3(2):129-38.
25. Gladney HM. Trustworthy 100-year digital objects: evidence after every witness is dead. *ACM Transactions on Information Systems (TOIS)*, 2004;22(3):406-36.
Abstract: In ancient times, wax seals impressed with signet rings were affixed to documents as evidence of their authenticity. A digital counterpart is a message authentication code fixed firmly to each important document. If a digital object is sealed together with its own audit trail, each user can examine this evidence to decide whether to trust the content---no matter how distant this user is in time, space, and social affiliation from the document's source. We propose an architecture and design that accomplish this: encapsulation of digital object content with metadata describing its origins, cryptographic sealing, webs of trust for public keys rooted in a forest of respected institutions, and a certain way of managing information identifiers. These means will satisfy emerging needs in civilian and military record management, including medical patient records, regulatory records for aircraft and pharmaceuticals, business records for financial audit, legislative and legal briefs, and scholarly works. This is true for any kind of digital object, independent of its purposes and of most data type and representation details, and provides every kind of user---information authors and editors, librarians and collection managers, and information consumers---with autonomy for implied tasks. Our prototype will conform to applicable standards, will be interoperable over most computing bases, and will be compatible with existing digital library software. The proposed architecture integrates software that is mostly available and widely accepted.



26. Gladney HM, Lorie RA. Trustworthy 100-year digital objects: durable encoding for when it's too late to ask. 2005.
Abstract: How can an author store digital information so that it will be reliably intelligible, even years later when he or she is no longer available to answer questions? Methods that might work are not good enough; what is preserved today should be reliably intelligible whenever someone wants it. Prior proposals fail because they generally confound saved data with irrelevant details of today's information technology---details that are difficult to define, extract, and save completely and accurately. We use a virtual machine to represent and eventually to render any data whatsoever. We focus on a case of intermediate difficulty---an executable procedure---and identify a variant for every other data type. This solution might be more elaborate than needed to render some text, image, audio, or video data. Simple data can be preserved as representations using well-known standards. We sketch practical methods for files ranging from simple structures to those containing computer programs, treating simple cases here and deferring complex cases for future work. Enough of the complete solution is known to enable practical aggressive preservation programs today.
27. Gladney HM. Trust and authenticity. Preserving digital information. 1 ed. Berlin: Springer; 2007. p. 93-107.
28. Gladney HM. Principles for digital preservation. Communications of the ACM 2007;49(2):111-6.
Abstract: Focusing on end users' needs rather than those of archiving institutions.
29. Glaeser EL, Laibson DI, Scheinkman JA, Christine L. Measuring trust. The Quarterly Journal of Economics 2000;115(3):811-46.
Abstract: We combine two experiments and a survey to measure trust and trustworthiness- two key components of social capital. Standard attitudinal survey questions about trust predict trustworthy behavior in our experiments much better than they predict trusting behavior. Trusting behavior in the experiments is predicted by past trusting behavior outside of the experiments. When individuals are closer socially, both trust and trustworthiness rise. Trustworthiness declines when partners are of different races or nationalities. High status individuals are able to elicit more trustworthiness in others.
30. Grandison T, Sloman M. A survey of trust in internet applications. IEEE communications survey: the electronic magazine of original peer-reviewed survey articles 2000;4:1-16.
31. Hank C. Digital curation and trusted repositories, seeking success JCDL 2006 workshop report. D-Lib Magazine 2006;Volume 12 Number 7/8.
32. Heery, Rachel and Anderson, Sheila. Digital repositories review. 2005. UKOLN.
Ref Type: Report
33. Heery, Rachel and Powell, Andy. Digital repositories roadmap: looking forward. 1-21. 2006. University of Bath, UKOLN, Eduserv.
Ref Type: Report
34. Huang J, Fox MS. An ontology of trust: formal semantics and transitivity. 2006.
Abstract: This paper formalizes the semantics of trust and studies the transitivity of trust. On the Web, people and software agents have to interact with "strangers". This makes trust a crucial factor on the Web. Basically trust is established in interaction between two entities and any one entity only has a finite number of direct trust relationships. However,



activities on the Web require entities to interact with other unfamiliar or unknown entities. As a promising remedy to this problem, social networks-based trust, in which A trusts B, B trusts C, so A indirectly trusts C, is receiving considerable attention. A necessary condition for trust propagation in social networks is that trust needs to be transitive. However, is trust transitive? What types of trust are transitive and why? There are no theories and models found so far to answer these questions in a formal manner. Most models either directly assume trust transitive or do not give a formal discussion of why trust is transitive. To fill this gap, this paper constructs a logical theory of trust in the form of ontology that gives formal and explicit specification for the semantics of trust. Based on this formal semantics, two types of trust -- trust in belief and trust in performance are identified, the transitivity of trust in belief is formally proved, and the conditions for trust propagation are derived. These results give theoretical evidence to support making trust judgment using social networks on the Web.

Notes: ISBN 1595933921

35. Jantz R, Giarlo MJ. Digital preservation: architecture and technology for trusted digital repositories. *D-Lib Magazine* 2005;11(6).
Abstract: Developing preservation processes for a trusted digital repository will require the integration of new methods, policies, standards, and technologies. Digital repositories should be able to preserve electronic materials for periods at least comparable to existing preservation methods. Modern computing technology in general is barely fifty years old and few of us have seen or used digital objects that are more than ten years old. While traditional preservation practices are comparatively well-developed, lack of experience and lack of consensus raise some questions about how we should proceed with digital-based preservation processes. Can we preserve a digital object for at least one-hundred years? Can we answer questions such as "Is this object the digital original"? or "How old is this digital object"? What does it mean to be a trusted repository of digital materials? A basic premise of this article is that there are many technologies available today that will help us build trust in a digital preservation process and that these technologies can be readily integrated into an operational digital preservation framework.
36. Jantz R. Digital preservation architecture and technology for trusted digital repositories. *D-Lib Magazine* 2005;Volume 11 Number 6.
37. Jantz R, Giarlo M. Digital archiving and preservation: technologies and processes for a trusted repository. *Journal of Archival Organization* 2007;4(1-2):193-213.
Abstract: This article examines what is implied by the term "trusted" in the phrase "trusted digital repositories." Digital repositories should be able to preserve electronic materials for periods at least comparable to existing preservation methods. Our collective lack of experience with preserving digital objects and consensus about the reliability of our technological infrastructure raises questions about how we should proceed with digital-based preservation practices, an emerging role for academic libraries and archival institutions. This article reviews issues relating to building a trusted digital repository, highlighting some of the issues raised and possible solutions proposed by the authors in their work of implementing and acculturating a digital repository at Rutgers University Libraries.
38. Jeffries FL. Subjective norms, dispositional trust, and initial trust development. *Journal of Behavioral and Applied Management* 2002;3(2):129-38.
Abstract: A model based on the generally accepted concept of the development of initial trust is tested. Subjective norms are included in the model in addition to dispositional trust and perceptions of the other's behavior. The findings show that dispositional trust is not influential on the development of an initial level of trust and an explanation grounded in the literature is offered. Subjective norms are influential however as soon as perceptions



of the other's behavior are available subjective norms' effect becomes insignificant. Perception of the other's behavior is the only significant influence on trust after a period of interaction between the participants. The findings are discussed and future research directions are offered.

39. Kaczmarek JS, Habing TG, Eke J. Repository software evaluation using the audit checklist for certification of trusted digital repositories. Chapel Hill, NC: 2006.
Abstract: The NDIIPP ECHO DEpository project [1] digital repository evaluation will use an augmented version of the draft Audit Checklist for Certification of Trusted Digital Repositories (Audit Checklist) [2] to provide a framework for examining how well currently popular repository software applications support the notion of a "trusted digital repository." The evaluation will also demonstrate the application of a scoring software evaluation methodology similar to one developed by the Center for Data Insight (CDI) at Northern Arizona University [3], used for evaluation data mining software. This scoring methodology in conjunction with the Audit Checklist can be used as a tool by librarians, archivists, and other data custodians to make informed decisions as they develop digital preservation management services.
40. Lewis DJ, Weigert A. Trust as a social reality. *Social forces* 1985;63(4):967-85.
41. Löfstedt RE. Introduction. Risk management in post-trust societies. Palgrave Macmillan; 2005.
Notes: Biographical note: RAGNAR E. LÖFSTEDT is Professor and Director of the King's Centre for Risk Management, King's College London and Adjunct Professor at Carnegie Mellon, Harvard and Gothenburg Universities. He is the editor and chief of the *Journal of Risk Research* and he has published/edited nine books and more than forty peer-reviewed articles. In December 2000 he was the first non-American awarded the Chauncey Starr award for exceptional contributions to the field of risk analysis for someone under the age of 40, by the Society for Risk Analysis.
42. Lynch CA. When documents deceive: trust and provenance as factors for information retrieval in a tangled web. *Journal of the American Society for Information Science and Technology* 2001;52(1):12-7.
43. Lynch, Clifford A. Institutional repositories: essential infrastructure for scholarship in the digital age. 226. 2003. ARL Association of Research Libraries. ARL: A Bimonthly Report, no. 226 (February 2003).
Ref Type: Report
Notes: Executive Director, Coalition for Networked Information
44. MacNeil H. Subject access to archival fonds: balancing provenance and pertinence. *Fontes Artis Musicae* 1996;43(3):242-58.
Abstract: Contribution to an issue devoted to Archives and music libraries. Traditionally access to archival fonds has been achieved by means of the provenance method, an indirect approach to subject access. However, subject indexing, a direct approach to achieving subject access and based on the principle of pertinence, has found favour recently in the archival community with a stronger inclination to reconcile provenance and pertinence based approaches to subject access. Discusses the 2 stages of the indexing process looking firstly at archival issues and trends relevant to the conceptual analysis of an archival fonds and secondly at issues relevant to translating indexing concepts into the terms of a controlled vocabulary.



45. MacNeil H. Providing grounds for trust: developing conceptual requirements for the long term preservation of authentic electronic records. *Archivaria* 2000;50(Fall):52-78.
Abstract: Since 1999 the International Research in Permanent Records in Electronic Systems (InterPARES) Project has been investigating the issues associated with the long term preservation of authentic electronic records. The identification of conceptual requirements for the verification of authentic electronic records is the responsibility of the InterPARES Task Force. There are three stages to the taskforce (1) identifying and defining, using contemporary archival diplomatics, the elements of an electronic record that are relevant to a consideration of authenticity (2) testing the validity of the elements through case studies of electronic systems, and (3) developing general and specific requirements for the preservation of electronic records over the long term. This article reports on the work accomplished by the task force to date in each of the three stages.
46. MacNeil H. Trusting records in a post-modern world. *Archivaria* 2001;51:36-47.
47. MacNeil H. Providing grounds for trust II: the findings of the InterPARES authenticity task force. *Archivaria* 2002;54:24-58.
48. McGuinness DL, Zeng H, et al. Investigations into trust for collaborative information repositories: a Wikipedia case study. 2007.
Notes:
Models of Trust for the Web (MTW'06) A workshop at the 15th International World Wide Web Conference (WWW2006), May 22-26, 2006, Edinburgh, Scotland
49. McHugh, Andrew, Ruusalepp, Raivo, Ross, Seamus, and Hoffman, Hans. Digital repository audit method based on risk assessment: DRAMBORA - draft for public testing and comment. 2007. Digital Curation Coalition (DCC), DigitalPreservationEurope (DPE).
Ref Type: Report
Abstract: DCC/DPE Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) provides a methodological framework, guidelines and audit tools to support the identification, assessment and managing of risks in a digital repository.
Notes: version 1.0 (draft)
50. Moore R, Smith M. Assessment of RLG Trusted Digital Repository Requirements. 2006 June 11; Chapel Hill, NC, USA: 2006.
51. Noda J, Takahashi M, Hosomi I. Integrating presence inference into trust management for ubiquitous systems. 2006.
Abstract: We propose a new architecture for trust management in ubiquitous environments that deals with RBAC policy, digital signatures, and user presence in a uniform framework. The proposed architecture includes inferences about user presence from incomplete sensor signals based on the hidden Markov model. We implemented a prototype system for a connection service in an office computer network with an RFID tag sensor system. Experimental results show that the proposed architecture is effective in providing both useful and secure services in a ubiquitous environment.
Notes: ISBN 1595933530
52. OCLC, CRL, and NARA. Trustworthy repositories audit and certification: criteria and checklist - version 1. 2007. Dublin Ohio, OCLC and CRL.
Ref Type: Report
Notes: Known as Trac



53. Patel A, al. Trust and privacy in digital business: first international conference, TrustBus 2004, Zaragoza, Spain. 2004 Aug. 30; Springer; 2004.
54. Reagle JMJ. Trust in electronic markets: the convergence of cryptographers and economists. *First Monday* 2005;Special issue no.3 5 Dec 2005.
Abstract: Relative to information security and electronic commerce, trust is a necessary component. Trust itself represents an evaluation of information, an analysis that requires decisions about the value of specific information in terms of several factors. Methodologies are being constructed to evaluate information more systematically, to generate decisions about increasingly complex and sophisticated relationships. In turn, these methodologies about information and trust will determine the growth of the Internet as a medium for commerce.
55. Reichherzer T, Brown G. Digital preservation, in, *Proceedings of the 6th ACM/IEEE-CS joint conference on Digital libraries* Chapel Hill. Chapel Hill, North Carolina: 2006.
Notes: ISBN 1595933549
56. Research Libraries Group. *Trusted digital repositories: attributes and responsibilities - an RLG-OCLC report.* 1-70. 2002. Mountain View CA.
Ref Type: Report
57. Research Libraries Group. *An audit checklist for the certification of trusted digital repositories: draft for public comment.* 2005. Mountain View, CA.
Ref Type: Report
58. Riegelsberger J, Sasse AM, McCarthy JD. The mechanics of trust: a framework for research and design. *International Journal of Human-Computer Studies* 2005;62(3):381-422.
59. Riegelsberger J, Vasalou A. *Trust 2.1: advancing the trust debate.* 2007.
Abstract: Trust has a considerable research tradition in the CHI community. It has been investigated in the context of e-commerce, virtual teams, online gaming, social networking to name a few. In this paper, we give an overview on this research. We delineate existing research along the key dimensions of objects of trust and related risks, methods and background of research, models of trust, and goals of trust research. Our aim is to provide a basis for the discussion at a special interest group (SIG), but also to give researchers and practitioners with an interest in the field an entry point to existing work. More importantly we hope that the SIG and this abstract will help in driving and structuring future trust research.
Notes: ISBN 9781595936424
60. RLG. *Attributes of a trusted digital repository: meeting the needs of research resources - draft for public comment.* 2002. Mountain View, California, RLG OCLC.
Ref Type: Report
61. Ross S, McHugh A. The role of evidence in establishing trust in repositories. *D-Lib Magazine* 2006;12(7/8).
62. Seadle M, Greifeneder, Elke. In archiving we trust: results from a workshop at Humboldt University in Berlin. *First Monday* 2008;13(1).
Abstract: If 25 specialists in preserving scholarly information had sat together in June of 1907 at the University of Berlin on Unter den Linden, they could likely have agreed that materials stored in the libraries of one of the world's great research universities in the



capitol of the richest and most powerful state in Europe could reasonably be trusted to survive long term. One hundred years later, after the events of the twentieth century had assaulted the collections with fire, water, looters, and censorship, representatives of four digital archiving systems came together to discuss the strengths and weaknesses of their systems face-to-face in front of an audience of librarians, who would have to choose whether any of these systems could be trusted to overcome the unknown events of the twenty-first century. A key conclusion was the need for interoperability and to pool efforts. An alternative to collaboration may be to let archiving systems compete on price, performance and advertising, but then as customers in that market, libraries need to think about how we can test long-term archiving, so that we have real evidence to decide whether the claims of reliability make sense.

63. Sillence E, Briggs P, Harris P, et al. A framework for understanding trust factors in web-based health advice. *International Journal of Human-Computer Studies* 2006;64(8):697-713.

Abstract: Trust is a key factor in consumer decisions about website engagement. Consumers will engage with sites they deem trustworthy and turn away from those they mistrust. In this paper, we present a framework for understanding trust factors in web-based health advice. The framework is derived from a staged model of trust and allows predictions to be made concerning user engagement with different health websites. The framework is then validated via a series of qualitative, longitudinal studies. In each study, genuine consumers searched online for information and advice concerning their specific health issue. They engaged in free searching and were directed towards sites previously reviewed using the framework. Thematic analysis of the group discussions provided support for the framework and for the staged model of trust wherein design appeal predicted *rejection* (mistrust) and credibility of information and personalization of content predicted *selection* (trust) of advice sites. The results are discussed in terms of the merits of the framework, its limitations and directions for future work.

64. Slovic P. Trust, emotion, sex, politics, and science: surveying the risk-assessment battlefield. *Risk Analysis* 1999;14(1):689-701.

Abstract: Risk management has become increasingly politicized and contentious. Polarized views, controversy, and conflict have become pervasive. Research has begun to provide a new perspective on this problem by demonstrating the complexity of the concept "risk" and the inadequacies of the traditional view of risk assessment as a purely scientific enterprise. This paper argues that danger is real, but risk is socially constructed. Risk assessment is inherently subjective and represents a blending of science and judgment with important psychological, social, cultural, and political factors. In addition, our social and democratic institutions, remarkable as they are in many respects, breed distrust in the risk arena. Whoever controls the definition of risk controls the rational solution to the problem at hand. If risk is defined one way, then one option will rise to the top as the most cost-effective or the safest or the best. If it is defined another way, perhaps incorporating qualitative characteristics and other contextual factors, one will likely get a different ordering of action solutions. Defining risk is thus an exercise in power. Scientific literacy and public education are important, but they are not central to risk controversies. The public is not irrational. Their judgments about risk are influenced by emotion and affect in a way that is both simple and sophisticated. The same holds true for scientists. Public views are also influenced by worldviews, ideologies, and values; so are scientists' views, particularly when they are working at the limits of their expertise. The limitations of risk science, the importance and difficulty of maintaining trust, and the complex, sociopolitical nature of risk point to the need for a new approach—one that focuses upon introducing more public participation into both risk assessment and risk decision making in order to make the decision process more democratic, improve the



relevance and quality of technical analysis, and increase the legitimacy and public acceptance of the resulting decisions.

65. Song S, JaJa J. Control and integrity: New techniques for ensuring the long term integrity of digital archives. 2007.
Abstract: A large portion of the government, business, cultural, and scientific digital data being created today needs to be archived and preserved for future use of periods ranging from a few years to decades and sometimes centuries. A fundamental requirement of a long term archive is to ensure the integrity of its holdings. In this paper, we develop a new methodology to address the integrity of long term archives using rigorous cryptographic techniques. Our approach involves the generation of a small-size integrity token for each digital object to be archived, and some cryptographic summary information based on all the objects handled within a dynamic time period. We present a framework that enables the continuous auditing of the holdings of the archive depending on the policy set by the archive. Moreover, an independent auditor will be able to verify the integrity of every version of an archived digital object as well as link the current version to the original form of the object when it was ingested into the archive. We built a prototype system that is completely independent of the archive's underlying architecture, and tested it on large scale data. We include in this paper some preliminary results on the validation and performance of our prototype.
Notes: ISBN 1595935991
66. Song S, JaJa J. New techniques for ensuring the long term integrity of digital archives. Philadelphia, Pennsylvania: Digital Government Society of North America; 2007.
Abstract: A large portion of the government, business, cultural, and scientific digital data being created today needs to be archived and preserved for future use of periods ranging from a few years to decades and sometimes centuries. A fundamental requirement of a long term archive is to ensure the integrity of its holdings. In this paper, we develop a new methodology to address the integrity of long term archives using rigorous cryptographic techniques. Our approach involves the generation of a small-size integrity token for each digital object to be archived, and some cryptographic summary information based on all the objects handled within a dynamic time period. We present a framework that enables the continuous auditing of the holdings of the archive depending on the policy set by the archive. Moreover, an independent auditor will be able to verify the integrity of every version of an archived digital object as well as link the current version to the original form of the object when it was ingested into the archive. We built a prototype system that is completely independent of the archive's underlying architecture, and tested it on large scale data. We include in this paper some preliminary results on the validation and performance of our prototype.
Notes: 1595935991
67. Suryanarayana G, Diallo MH. Architecting trust-enabled peer-to-peer file-sharing applications. *Crossroads* 2006;12(4):5.
Abstract: Decentralized peer-to-peer (P2P) resource sharing applications lack a centralized authority that can facilitate peer and resource look-ups and coordinate resource sharing between peers. Instead, peers directly interact and exchange resources with other peers. These systems are often open and do not regulate the entry of peers into the system. Thus, there can be malicious peers in the system who threaten others by offering Trojan horses and viruses disguised as seemingly innocent resources. Several trust-based solutions exist to address such threats; unfortunately there is a lack of design guidance on how these solutions can be integrated into a resource sharing application. In this paper, we describe how two teams of undergraduate students separately integrated XREP, a third-party reputation-based protocol for file-sharing applications, with PACE, our software architecture-based approach for decentralized trust management. This was



done in order to construct trust-enabled P2P file-sharing application prototypes. Our observations have revealed that using an architecture-based approach in incorporating trust into P2P resource-sharing applications is not only feasible, but also significantly beneficial. Our efforts also demonstrate both the ease of adoption and ease of use of the PACE-based approach in constructing such trust-enabled decentralized applications.

68. Thibodeau K. What constitutes a success in a digital repository? 2006.
Notes: June 11-15, 2006 — Chapel Hill, NC, USA
69. Tyler O.Walters, Robert H.McDonald. Creating trust relationships for distributed digital preservation federations. 2008 Aug. 29; London: British Library; 2008.
70. Van House NA. Trust and epistemic communities in biodiversity data sharing. 2002.
Abstract: Trust is a key element of knowledge work: what we know depends largely on others. This paper discusses the concepts of communities of practice and epistemic cultures, and their implication for design of digital libraries that support data sharing, with particular reference to practices of trust and credibility. It uses an empirical study of a biodiversity digital library of data from a variety of sources to illustrate implications digital library design and operation. It concludes that diversity and uncomfortable boundary areas typify, not only digital library user groups, but the design and operation of digital libraries.
Notes: ISBN 1581135130
71. Viklund MJ. Trust and risk perception in Western Europe: a cross-national study. Risk Analysis 2003;23(4):727-38.
Abstract: The relationship between trust and risk perception was investigated, within and across four European countries (Sweden, Spain, United Kingdom, and France). Survey data were collected in 1996; total number of respondents was approximately 1,000 (United Kingdom and Spain), 1,350 (France), and 2,050 (Sweden). Trust was a significant predictor of perceived risk within countries, but the strength of the relationship varied from weak (Spain and France) to moderate (United Kingdom and Sweden). General trust was also a significant source of variation in perceived risk among countries, but much of the variation in perceived risk remained unexplained. Correlations between trust and risk perception also varied depending on the type of risk (i.e., nuclear risks were more influenced by trust) and trust measure (i.e., general trust explained perceived risk better than specific trust). It is concluded that trust may be an element in models explaining risk perception, but it is not as powerful as often argued in the risk perception literature.



A. APPENDIX 1

CASPAR Trust and digital repositories questionnaire

CASPAR - Cultural, Artistic and Scientific knowledge for Preservation, Access and Retrieval - an Integrated Project co-financed by the European Union within the Sixth Framework Programme (Priority IST-2005-2.5.10, "Access to and preservation of cultural and scientific resources"). For more information please see <http://www.casparpreserves.eu/>

As part of CASPAR’s research activity we are investigating notions of trust with regard to digital repositories. We very much appreciate you taking the time to answer these questions on trust in relation to digital repositories as this will help to build understanding of what trust means to various communities.

Section 1 – questions about you

1) Which organisation/domain are you associated with?

Please put an ‘x’ by the one which applies to you.

- a) Performing arts (music, scenography, choreography...)
- b) UNESCO – cultural heritage
- c) ESA-ESRIN - science

2) What is your job title and role?

.....
.....

3) What is your main role in the digital curation lifecycle?

Please put an ‘x’ by the one(s) which best apply to you

- a) Creator of digital objects
- b) Curator of digital objects
- c) User of curated digital objects

Section 2 - questions about repositories

How important are the following factors when deciding if a digital repository is trustworthy?

Please indicate the level of importance where 0 is not important and 5 is very important

4) Personal contact with staff at a repository (you know someone who works there)



0 1 2 3 4 5

5) Personal recommendation (a colleague tells you about it)

0 1 2 3 4 5

6) Recommendation through professional network (email discussion lists, conferences and seminars, journal/magazine articles)

0 1 2 3 4 5

7) Track record of the repository's ability to curate objects and to provide reliable efficient access to authentic objects over time (examples of the repositories' previous work)

0 1 2 3 4 5

8) The repository preserves the audit trail and documents the preservation processes. The repository can demonstrate reliable and efficient access to authentic objects over time.

0 1 2 3 4 5

9) The control of integrity within the repository (e.g. digest, checksum, digital signature, other)

0 1 2 3 4 5

10) Repository conformity to international or national standards

0 1 2 3 4 5

Which standards in particular?

Please put a 'x' by those that apply

- ISO 9001:2000 Quality management systems
- ISO/IEC 17799:2005 Information technology. Security techniques. Code of practice for information security management
- ISO/IEC 27001:2005 Information technology. Security techniques. Information security management systems
- ISO 15489-1:2001 Information and documentation. Records management. General
- ISO 23081-1:2006 Information and documentation -- Records management processes -- Metadata for records
- ISO11799 : 2003 Information and documentation - Storage requirements for archive and library materials
- or sector standards such as



- CIDOC/CRM (international museums)
- Spectrum (UK museum)
- Others – please list.....

11) Repository has been validated by a toolkit such as Digital Repository Audit Based on Risk Assessment (DRAMBORA), or Trusted Repositories Audit Criteria (TRAC)

Please indicate the level of importance where 0 is not important and 5 is very important

0 1 2 3 4 5

12) Repository has been validated by a domain-specific authority such as the Museums Documentation Association (MDA)

0 1 2 3 4 5

Please specify.....

13) Physical security of the repository building

0 1 2 3 4 5

14) Security of the contents of the repository (e.g. the objects are secured against corruption – either intentional or unintentional)

0 1 2 3 4 5

15) Marketing and passion

0 1 2 3 4 5

16) The repository has well defined plans relating to its governance and operations.

Yes No

If 'Yes' please indicate the importance of the following plans.

a) Business plan

0 1 2 3 4 5

b) Acquisition plan



0 1 2 3 4 5

c) Staffing plan

0 1 2 3 4 5

d) Access plan

0 1 2 3 4 5

e) Technical plan

0 1 2 3 4 5

f) Data plan

0 1 2 3 4 5

g) Succession plan (for after the repository ceases to exist)

0 1 2 3 4 5

h) Disaster plan

0 1 2 3 4 5

i) Preservation plan

0 1 2 3 4 5

17) Are there any other elements which help you decide if a repository is trustworthy? If so please describe them below.

.....

.....