RLG DigiNews
RLG's online newsletter for digital imaging and preservation

> Feature Article 1

**Audit and Certification of Digital Repositories: Creating a Mandate for the Digital Curation Centre (DCC)**

Authors: Seamus Ross (s.ross@hatii.arts.gla.ac.uk), Andrew McHugh (A.McHugh@hatii.arts.gla.ac.uk)

**Introduction to the problem**

If digital repositories are to remain viable, trust and the closely related issue of quality assurance must both be tackled as overarching priorities. Every step towards this end must gracefully fit within an existing context that includes standards for quality assurance (ISO 9000 series), information security (ISO 17799:2005), institutional records management (ISO 15489:2001), and the Open Archival Information Systems Reference Model (OAIS, ISO 14721).

With the increasing volume of digital information being created across contemporary organisations, businesses, and academic institutions, it is inevitable that the need for reliable digital storage and management services has experienced commensurate growth. [1] Digital information, by its very nature, is prone to change, and the ease with which digital information can be manipulated and altered is cited in many contexts as one of its great strengths. But its flexibility can be just as straightforwardly interpreted as a vulnerability, and the passage of time presents challenges to the maintenance of its usability, authenticity, integrity, and reliability. These issues prompted the Task Force on Archiving of Digital Information to assert in 1996 that "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."[2] Fundamental to the value of digital repositories is their trustworthiness and ability to accommodate (possibly a wide range of) digital information, ensure its security, guarantee its authenticity, and facilitate its accessibility and usability. Several classes of trust relationships are involved in the numerous interactions that surround any digital repository. *Trusted Digital Repositories: Attributes and Responsibilities* (Research Libraries Group and the Online Computer Library Center (2002)) describes a minimum of three levels: how information holders earn the trust of their designated communities, how information holders trust third-party service providers, and how users trust digital assets provided to them by a repository. [3] If digital repositories are to remain viable, trust and the closely related issue of quality assurance must both be tackled as overarching priorities. Every step towards this end must gracefully fit within an existing context that includes standards for quality assurance (ISO 9000 series) [4], information security (ISO 17799:2005) [5], institutional records management (ISO 15489:2001) [6], and the Open Archival Information Systems Reference Model (OAIS, ISO 14721). [7]

**What must a repository be able to do?**

A range of trust-related issues surrounds digital repositories. Expectations of users and depositors, aspirations of service providers, and management concerns all must be addressed. Many characteristics can be identified as necessary for most, if not all, digital repositories. Security must be watertight. Controls must exist to protect and provide a guarantee for the authenticity and integrity of stored materials; accessibility must be maintained; and documentation, metadata, and assets must all be self-contained and maintained in-house or in other trusted repositories. The repository must be clear about the data types and formats it can handle. Disaster recovery measures should be incorporated from the beginning and exit strategies conceived at the time the organisation is established. In many ways, *digital curation and preservation is a risk management activity at all stages of the longevity pathway*. With the

temporal dimension implicit in the remit of digital repositories, it is vital that repositories are equipped to deal with the inevitable changes that will occur over time. The passage of time is manifested in the need to refresh storage technologies, maintain verification systems, define comprehensive and flexible workflows, and adopt a reactive and flexible approach to service provision. Other key areas of risk include management and, especially, management continuity, preservation policies, organisational structures, and approaches to sustainability. Furthermore, long-term repositories must accommodate the outcomes and effects of preservation actions such as migration and emulation and accommodate the use of newer approaches as they emerge. If the repository claims to be preserving information, rather than just bit streams, then the understandability and usability of its holdings must also be sustained.

A digital repository must be able to ensure that the information it holds and makes accessible is what it purports to be–that is, any subsequent instantiation of a digital record or asset needs to share the same content, functionality, and behaviour as the initial instantiation. Authenticity can be assured only with the application of strict ingest controls and the documentation and the preservation of any significant properties throughout any subsequent migrations or application of other preservation actions. [8] Additionally, a successful archive must also be able to offer assurances of information integrity. Distinct from authenticity this means ensuring that the digital entity is intelligible, understandable, and/or usable by the associated designated community. Security measures are one mechanism a repository can use to mitigate problems associated with maintaining information integrity. Security is a challenge; even in traditional repositories it has posed difficulties. We are reminded of John Myatt, a prolific forger whose success lay not in his painting but in the ability of his colleague John Drewe to create provenance for his forgeries, including works of Braque, Matisse, Giacometti, Chagall, and Le Corbusier. The forgeries were good, but it was the fabricated provenances for them that made it possible for the works to be sold by respected art dealers in London and New York and auction houses including Christie's and Sotheby's. John Drewe "systematically infiltrated some of the most security-conscious art archives in the world, altering the provenances of genuine paintings to establish a lineage making way for Myatt's mostly unexceptional forgeries." [9] Trusted national repositories in the UK, such as the Victoria and Albert's National Art Library, the Institute of Contemporary Art in London, and the Tate Library's archives, all provided him with unrestricted access to their holdings. Peter Landesman reported that "Drewe changed and fabricated so many records at both the Victoria and Albert and the Tate, and with so many different artists, that the directors of both museums admit that they may never know how much of their collection has been corrupted." [10] Ensuring security in the digital repository is not merely a technological problem, but just as in the traditional archival environment security, it is a cultural, political, and social challenge that organisations must meet.

We are reminded of John Myatt, a prolific forger whose success lay not in his painting but in the ability of his colleague John Drewe to create provenance for his forgeries, including works of Braque, Matisse, Giacometti, Chagall, and Le Corbusier.

**What conditions must be satisfied to attain trusted status?**

There is a range of ways in which digital repositories must engender, establish, and maintain trusted status. In some circumstances, information holders or service providers may already be regarded, by experience or reputation, as trustworthy. In many more cases, information holders are unable to refer to a long history of success in the handling of digital resources and must adopt new ways to demonstrate their competence and reliability. Some institutions, such as national libraries and archives, already have achieved trusted status in the traditional paper environment and there is a general expectation that they "will develop and continue to fulfil this role in the digital environment." [11] Compared to institutions and organisations in other sectors they certainly do have an enviable track record in managing heritage assets. The contrast is highlighted when we reflect on Reed-Elsevier's decision to delete from its digital store some articles that it had published; of course, this raises concerns and it left at least one academic wondering: "What guarantors other than libraries do we realistically have?" [12] But why on earth should we implicitly trust public sector organisations such as national libraries or archives to perform functions that are new, untested, and in a territory that is organisationally and culturally uncharted? The new environment will require all players to establish their "trusted" status. How can this be done? In reality there are several questions that can be posed relating to the establishment and maintenance of trusted status. How is trust initially established? What is required in order to sustain it? Can it be secured and, if so, how? In the event that trust is lost can it be re-acquired? Perhaps most importantly, how can trust be verified and a repository assert its own status as "trusted"? Most issues of trust stem from procedural effectiveness.

Why on earth should we implicitly trust public sector organisations such as national libraries or archives to perform functions that are new, untested, and in a territory that is organisationally and culturally uncharted?

*Attributes and Responsibilities* describes attributes that a repository must have in order to claim trusted status. These include Open Archival Information System (OAIS)[13] compliance, administrative responsibility, organisational viability, financial sustainability, technological and procedural suitability, and system security and procedural accountability. Acceptable performance in all these areas will be achieved by (among other things) establishing transparent and executable policies and procedures, meeting standards for all aspects of security (including disaster recovery), defining a mission statement that makes explicit a commitment to the long term, promoting transparent business practice(s), adhering to a sound business plan, adopting appropriate and open technological solutions (e.g., hardware and software), and recording and justifying all preservation actions undertaken. Similarly, types of relationships with depositors, analyses of user needs, application of appropriate metadata processes, and mechanisms to manage and benchmark the quality of service also play a crucial role in repository effectiveness.

The RLG-NARA Digital Repository Certification Task Force has published a draft checklist for certifiable elements of a digital archive, and this represents an excellent starting point for considering what characteristics are fundamental.[14] However, other approaches have been suggested as well. For instance, can a non-OAIS compliant repository model ever be regarded as trusted?[15] Perhaps the answer will depend upon the nature of such frameworks and what the repository is being trusted to do. The RLG-NARA checklist is very broadly applicable.

The German Initiative for Networked Information (DINI) [16] and the Network of Expertise in Long-term STOrage of Digital Resources (nestor) [17] in Germany have both had considerable success determining certification criteria for document repositories (see companion article in this issue). In addition, The Committee of Sponsoring Organizations of the Treadway Commission (COSO) [18], Control Objectives for Information and Related Technologies (COBIT) [19], and IT Infrastructure Library (ITIL) [20] provide useful, albeit perhaps more generically IT-based, alternatives to the RLG-NARA approach. The first of these, COSO, supports the delivery of mechanisms to enhance the quality of financial reporting through business ethics, effective internal controls, and corporate governance. The second is an open standard IT Control framework for improving the delivery and management of information and associated technologies built on the COSO framework. The use and functionality of the COBIT framework is complemented by use of the IT Infrastructure Library. It should be noted that none of the above claim to certify the long-term preservation of information, however, each of these addresses one or more of the many aspects relevant to such preservation.

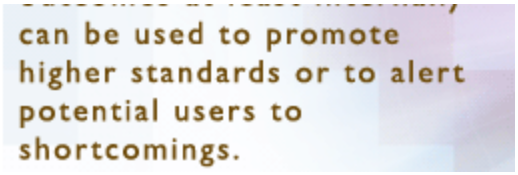
A crucial step in ensuring the take-up of trust-validating mechanisms is defining and agreeing on the benefits of and motivations for achieving a trusted status.

A crucial step in ensuring the take-up of trust-validating mechanisms is defining and agreeing on the benefits of and motivations for achieving a trusted status. Potential depositors, funders of content creation, and future users, whether these are persons or machines, all will expect that mechanisms will be in place that will enable them to determine whether they can trust a repository and then what level of trust they can accord it and in what contexts (e.g., for what data types). For their part, organisations may be motivated to use independent mechanisms for demonstrating their trusted status where: 1) having an indicator of trusted status is relevant to the organisation's mission and goals; 2) it helps them to achieve their business objective; 3) the balance between the costs of acquiring trusted status and the benefits accrued from such investment can be justified; or 4) a specific business case can be made (e.g., a potential high-value depositor or user requires such externally awarded markers of trust before being prepared to place digital objects in the repository).

**How can a repository formalise its trusted status?**

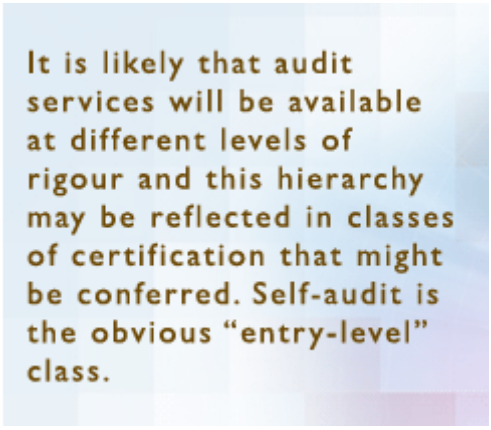
By undergoing an examination of their processes, infrastructure, and information-management competence, institutions, information holders, and service providers can obtain a trusted, certified status that provides a sense of reassurance to their various stakeholders. Conversely, where practices are of insufficient quality, audits can highlight this. Publishing the outcomes at least internally

With an understanding of what constitutes a trusted repository infrastructure, the next logical step is to identify how organisations can establish and convey their trustworthiness. Among the most favoured solutions is the introduction of a certification infrastructure for digital repositories. In their 1996 declaration in favour of the establishment of trusted archives, the Task Force on Archiving of Digital Information added that a trusted status could not simply be self-conferred, and that "a process of certification for digital archives is needed to create an overall climate of trust about the prospects of preserving digital information."[21] This ultimately necessitates the conception of some kind of auditing infrastructure consisting of 1) organisations to perform the assessment and confer appropriate certification and 2) a system for accreditation of such organisation. Such auditing activities present a number of challenges and raise several questions. The first concerns what an audit should seek to achieve.




By undergoing an examination of their processes, infrastructure, and information-management competence, institutions, information holders, and service providers can obtain a trusted, certified status that provides a sense of reassurance to their various stakeholders. Conversely, where practices are of insufficient quality, audits can highlight this. Publishing the outcomes at least internally can be used to promote higher standards or to alert potential users to shortcomings. As Hans Hofman of the Dutch National Archives commented, public release of the external audit reports would itself be a powerful mechanism, especially where it exposed weakness in particular repositories.

A less immediately obvious question is to ask what exactly should be audited, and the RLG-NARA draft audit checklist attempts to address this. Even where it is possible to identify the auditable aspects within a single repository, questions arise about which service providers or information holders should be audited or at least eligible to request such a service. Some organisations that might be likely to seek certification include national and major research libraries, archives and record management centres, data centres, and commercial service providers. Since very few organisations or projects have guaranteed funding for the indefinite future, we clearly would expect repositories, which are themselves ephemeral, but which are seen as part of a chain of preservation, to seek certification. The incentives and disincentives influencing an organisation's decision to undergo audit are likely to vary, though if relevant or integral to the missions or goals of the organisation, then audit and subsequent certification is likely to be desirable. Similarly, if customers identify certification as a persuasive factor in choosing a service provider it may be a necessary procedure from a business point of view. It is possible that certification may become a legal obligation for some institutions in order for them to continue to operate in particular regulatory environments. Of course, if the procedures that are introduced prove too costly or complex then these are likely to act as a disincentive. Ultimately, assuming that most organisations will not face obligatory audits, decisions will be based on a subjective cost-versus-benefit projection.




It is likely that audit services will be available at different levels of rigour and this hierarchy may be reflected in classes of certification that might be conferred. Self-audit is the obvious "entry-level" class. This could be a useful internal process, and products like the RLG-NARA draft audit checklist can be used or extended to facilitate it. Self-audit may be a worthwhile way for an institution to prepare for a subsequent and more onerous external audit, or for some low-volume or low-risk repositories, it may be a sufficient benchmark. Effective use of self-audits could reduce the costs of external audits, for example, raising awareness of the kinds of documentation needed. Furthermore, the auditability of an individual institution is likely to be a significant factor in its perceived trustworthiness: self-examination based on pre-defined criteria is a useful way to enable institutions to adopt a best-practice mindset that will better equip them to face more intense scrutiny. The most in-depth external audits are likely to cover every aspect of a repository's business, including systems, finances, personnel, and procedures. It is unlikely that every repository will need to acquire formal certification if they are to achieve trusted status

The time frame of auditing should also be considered. It seems impossible that certification from a single audit should persist indefinitely. As with any other certification, one would expect regular re-certification audits, driven not least by the fundamental difference of this type of certification from all others–namely the "long-term" preservation that is required. Predefined events or quantitative performance triggers may also compel re-certification. Further decisions will have to be made to determine whether depositors or users will have the power to demand "surprise audits." Of course, this will depend on the means of the agency or agencies responsible for performing the audits and conferring certification or accreditation. Auditors will be expected to be both multi-disciplinary and independent (over a very long-term period) and command recognition from the communities they seek to serve. To make this work, an accreditation system would be expected to be in place, underpinned by international standards and consensus. Given the time scales involved, change will be a feature of the accreditation, certification, and audit processes.

A further question that remains is that of the logistics of the audits themselves. How in practice will these be conducted? Inevitably, a great deal of information will need to be made available to auditors in order for them to establish a useful understanding. As we have already noted, initial self-audits will enable institutions to ensure that their information infrastructures are sufficiently robust and suitably tailored to suit the rigours of external assessment. Policies, workflows, custody chain documentation, financial and human resource records, and systems data will be among the types of information sought by auditors. Objective conclusions will only be possible following the definition of measurable attributes, and, where currently unavailable, attempts will have to be made to define some kind of quantifiable targets. Relationships between the various communities involved will be analysed. Analysis of the needs of classes of users including producers and consumers will offer some insights into the success with which repositories have met their own remits. In addition, relationships between people and aspects of the system

functionality will likely come under scrutiny. For instance, one of several checks will be to establish the robustness of ingest mechanisms and the subsequent ability of the repository to sustain information authenticity and understandability.

**Gaining an audit and certification mandate**

What organisation or organisations can achieve a mandate to manage audit processes and to oversee the awarding of certified status? In the UK we hope that the Digital Curation Centre, working with national, European, and international bodies, can earn this mandate. The Digital Curation Centre has been funded for three years by the UK Joint Information Systems Committee (JISC) and the UK e-Science Core Programme of the Engineering and Physical Sciences Research Council (EPSRC),working in collaboration with professionals and organisations in the area of digital curation. [22] The DCC, led by a consortium of four institutions, each bringing diverse experience, [23] is the national focus for digital curation research and promotes expertise and good practice, both nationally and internationally, in the management of all research outputs in digital format. The Digital Curation Centre, through its organisation, emphasis, and practical activities, closely reflects these ideals and it aims to catalyse action in innovative research, development, service delivery, and outreach. The DCC promotes an understanding of the need for digital curation among the communities of scientists and scholars, it provides services to facilitate digital curation, it shares knowledge of digital curation among data creating and using disciplines, it develops technology in support of digital curation, and it leads innovative research in digital curation. Given the broadness and pervasiveness of the digital curation challenge, the core partners recognise that a sustainable contribution can only be made if widespread activity can be leveraged. To ensure that this happens the partners are working to develop a diverse network of associates, including individuals and organisations.

The Digital Curation Centre has established audit and certification as a key priority within both its research and service provision commitments.

The Digital Curation Centre has established audit and certification as a key priority within both its research and service provision commitments. This is manifesting itself in a wide range of activities: raising awareness of the needs and processes involved in audit; contributing to the validation of audit checklists; developing audit procedures and self-audit tools; participating in the debates surrounding audit controls and certification guidelines; and building accreditation consensus. We still have not come to terms with the costs: how much it will cost the DCC to conduct audits, what the cost implications for organisations wishing to undergo audit might be, and what tools we might use to determine the cost benefit relationships. As with other audit and certification processes, it is likely that external costs can be contained through having effective internal procedures in place.

Audit and certification fit alongside our already expansive array of training commitments. The DCC will support its implementation of audit and certification services through training events, targeted at information holders and service providers and aimed at offering insights into a range of activities and documentation needed to prepare for audit. Some examples include training on how to design repository infrastructures with certification in mind, on conducting internal self-audits, and on preparing for a fuller external audit. Eventually these training packages will be distributed online as virtual tutorials via the DCC's Web portal. In addition, the DCC will be publishing a tool to enable institutions to perform their own internal audits. Successful completion will result in eligibility for bronze level certification and provide an indication of institutional preparedness for higher-levels of certification. This tool will take the form of a series of assessable attributes, which can be identified and scored by institutions within their own repository infrastructures. Further services will see the DCC itself assume the role of auditor in the first instance to the UK's Higher and Further Education community and members of the DCC's own Network of Associates. Successful completion of these audits (which will be of varying intensity) will result in the award of silver and gold certification.

In parallel and in collaboration with RLG, the DCC will conduct two audits of scientific data repositories to test the RLG-NARA Checklist and as a capacity building exercise.

To help lay the foundation for these activities, the DCC is contributing to pilot audit studies that will begin over the coming months in the US and Europe. In parallel and in collaboration with RLG, the DCC will conduct two audits of scientific data repositories to test the RLG-NARA Checklist and as a capacity building exercise. These investigations have been designed to validate not just the appropriateness of the checklist, but to provide us with an understanding of the process and costs of its use as an audit tool. One problem is that we do not really know what skills an auditor must have and which ones they should have in this context. There is though an expectation that the ideal auditor would be independent, multi-disciplined (for example professional auditor and knowledgeable in ICT, law, workflow, and project management), and perhaps not a single individual but a team.

The DCC anticipates that the need is for a multi-tiered audit and certification programme (bronze, silver, and gold certificates), which is acknowledged by the major cultural and scientific heritage community in Europe to be the standard for assessing such services. This will be supported by publicly and freely accessible tools (both online and paper-based) to enable repositories and other data holding organisations to conduct self-audits. This approach will be combined with an effort to encourage the development by commercial and not-for-profit organisations of audit services in the arena of trusted repositories. The foundation of a consortium of repositories with certification at Gold and Silver that can act as a safety-net for repositories affected by changes in their status, mission, or funding environment whose collections may then be at risk, will also play an essential role in the eventual trust placed in any certification scheme. The possibility of constructing a network of trusted repositories may be viable in the UK as the JISC has recently funded twenty-five projects to a total of £3.2 million to "ensure the maximum degree of coordination in the development of digital repositories, in terms of their technical and social (including business) aspects."[24]

Underpinning all DCC services in this area is an ongoing commitment to research the issues within the scope of audit and certification that remain unresolved, ambiguous, or unclear (e.g., relevance of the RLG-NARA Checklist, mechanisms for establishing an internationally recognised audit and certification approach). Promotion of the merits of certification for all the involved parties including depositors, end users, repository managers, and third-party service providers is another key work area. By cooperating with those already experienced in the field and developing its own expertise and products, it is hoped that the DCC can make a significant contribution to the establishment of a more trustworthy digital repository landscape within the UK.

The prospect of the emergence of audit, certification, and accreditation mechanisms should not leave institutions like startled rabbits captivated by the glare of the headlights of the oncoming juggernaut. It is possible to act positively to lay a foundation of policies, practices, and services that will provide institutions with a level of preparedness for the eventual implementation of audit and certification mechanisms by the community. Prior to the wide availability of these services digital repositories can take a variety of preparatory steps. Examples include: defining and documenting the objectives and aims of the repository itself and of any services being provided; defining, documenting, and applying policies and procedures; developing management steering roles and responsibilities; maintaining risk registers, status reports, and minutes from meetings; and defining, implementing, and monitoring disaster recovery plans. Many of these steps will have already been undertaken in the ordinary course of business, but by refining these into a shape that is more easily auditable (in terms of the work that has already been done in the area) difficulties can be avoided in the future. Put simply, if repositories document what they say or do, have the capability to demonstrate that they *can* do what they say, and can show that they *do* do what they say, then they are likely to be performing effectively. In these cases audit should be welcomed.

*Acknowledgements*
The authors wish to thank their colleagues in the DCC and, on this occasion particularly, to acknowledge Adam Rusbridge and Yunhyong Kim for their advice. David Giaretta, also of the DCC, provided essential guidance and comments, although we did not reflect all his suggestions in the final version. We would like to thank Hans Hofman, of the Dutch National Archives, for his suggestions. Any errors that remain are, of course, our own.

*Citations:*
[1] S. Anderson and R. Heery, 2005, *Digital Repositories Review*.

[2] Commission on Preservation and Access and the Research Libraries Group, 1996. *Preserving Digital Information, Report of the Task Force on Archiving of Digital Information*, page 40 (last accessed, 10 Oct 2005).

[3] RLG/OCLC Working Group on Digital Archive Attributes, 2002, *Trusted Digital Repositories: Attributes and Responsibilities*. (last accessed, 10 Oct 2005).

[4] ISO Management Systems

[5] ISO/IEC 17799:2005: Information technology - Security techniques - Code of practice for information security management

[6] ISO 15489-1:2001 Information and documentation - Records management - Part 1: General, ISO/TR 15489-2:2001 Information and documentation - Records management -Part 2: Guidelines

[7] *Reference Model for an Open Archival Information System (OAIS) – ISO 14721,* 2002). (last accessed, 10 Oct 2005).

[8] *Integrity and Authenticity of Digital Cultural Heritage Objects*, 2002, DigiCULT Thematic Issue 1, and *The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project*, 2004,see the report of the "Authenticity Task Force",

[9] On the case see for example: "Art fraudster jailed", Monday, February 15, 1999 or P. Landesman, 1999, " A 20th-Century Master Scam", 18/07/1999,

[10] Landesman, 1999.

[11] S. Ross 2003, *Digital Library Development Review*, National Library of New Zealand,

(Wellington), ISBN: 0-477-02797-0. ,

[12] J. O'Donnell in a posting to *Liblicense-L* on 29 January 2003 (Subject "Re: vanishing act" ) (last access, 10 Oct 2005)

[13] *Reference Model for an Open Archival Information System (OAIS) – ISO 14721*, 2002). (last accessed, 10 Oct 2005). Although the authors would argue that any certification scheme will need to allow for other underlying models as they emerge.

[14] RLG-NARA Task Force on Digital Repository Certification: Audit Checklist for Certifying Digital Repositories, (last accessed, 10 Oct 2005). See article by Robin Dale in this issue.

[15] Further investigation may be needed to decide whether or not any audit, certification, and accreditation programme will need to be flexible enough to be responsive to future preservation models that may emerge. See for instance, D. S. H. Rosenthal, T. S. Robertson, T. Lipkis, V. Reich, and S. Morabito, 2005, "Requirements for Digital Preservation Systems: A Bottom-Up Approach"

[16] DINI, Deutsche Initiative für Netzwerkinformation eV

[17] NESTOR, Network of Expertise in Long-Term Storage of Digital Resources

[18] http://www.coso.org

[19] http://www.isaca.org/cobit

[20] http://www.ogc.gov.uk/index.asp?id=2261

[21] Commission on Preservation and Access and the Research Libraries Group, 1996. *Preserving Digital Information, Report of the Task Force on Archiving of Digital Information*, page 40, (last accessed, 10 Oct 2005).

[22] http://www.dcc.ac.uk For a more detailed description of the DCC and its work see C. Rusbridge, P. Burnhill, S. Ross, P. Buneman, D. Giaretta, L. Lyon, M. Atkinson, 2005, "The Digital Curation Centre: A Vision for Digital Curation", In *Proceedings IEEE"s Mass Storage and Systems Technology Committee Conference on From Local to Global: Data Interoperability--Challenges and Technologies*, an online version is at: http://eprints.erpanet.org/archive/00000082/01/DCC_Vision.pdf

[23] It brings together organisations across three Universities and a research council. Led by the University of Edinburgh [], which hosts the School of Informatics, the National eScience Centre (NeSC), the EDINA national data centre, the DCC consortium includes HATII [22] at the University of Glasgow Humanities Advanced Technology and Information Institute (HATII), UKOLN at the University of Bath, and the Council for the Central Laboratory of the Research Councils (CCLRC).

[24] JISC Digital Repositories Programme