The Role of Evidence in Establishing Trust in Repositories

Seamus Ross	Andrew McHugh
Visiting Fellow Oxford Internet Institute & Digital Curation Centre (DCC) & Humanities Advanced Technology and Information Institute George Service House, 11 University Gardens University of Glasgow Glasgow G12 8QQ +44 141 330 8592 s.ross@hatii.arts.gla.ac.uk	Digital Curation Centre (DCC) & Humanities Advanced Technology and Information Institute George Service House, 11 University Gardens University of Glasgow Glasgow G12 8QQ +44 141 330 8592 a.mchugh@hatii.arts.gla.ac.uk

ABSTRACT

This paper arises from work by the Digital Curation Centre (DCC) Working Group examining mechanisms to roll out audit and certification services for digital repositories in the United Kingdom. Our attempt to develop a program for applying audit and certification processes and tools took as its starting point the RLG-NARA *Audit Checklist for Certifying Digital Repositories* [8]. Our intention was to appraise critically the checklist and conceive a means of applying its mechanics within a diverse range of repository environments. We were struck by the realization that while a great deal of effort has been invested in determining the characteristics of a 'trusted digital repository', far less effort has concentrated on the ways in which the presence of the attributes can be demonstrated and their qualities measured. With this in mind we sought to explore the role of evidence within the certification process, and to identify examples of the types of evidence (e.g., documentary, observational, and testimonial) that might be desirable during the course of a repository audit.[1]

Categories and Subject Descriptors

H.3.7 [**Information Systems**]: Information Storage and Retrieval, Digital Libraries — *standards, system issues, user issues*.

General Terms

Management, Documentation, Reliability, Experimentation, Security, Legal Aspects, Verification.

Keywords

Trust, Repository, Evidence, Digital Preservation, Digital Curation.

1. INTRODUCTION

Digital repositories have become a focal point of institutional development [1]. Numerous activities from eprint services to institutional repositories to developments at national libraries and archives reflect the recognized need to develop, deploy, and maintain trusted digital repositories. The reasons why independently measuring and validating the trustworthiness of repositories is essential have been the focus of earlier discussions [5, 9, 10]. For the purposes of this study we have taken as axiomatic that certification is one marker that helps users to establish the level of trust that they might reasonably have in a particular digital repository. Audit is a critical step in establishing whether certification of a particular repository should be granted. Here we aim to open the debate on the types of evidence needed if digital repositories are to be effectively and transparently audited.

Funded jointly by the Joint Information Systems Committee (JISC)[2] and the core e-Science Programme, the Digital Curation Centre (DCC) aims to support and promote continuing improvement in the quality of data curation and digital preservation, within the United Kingdom. The four partners, the University of Edinburgh[3], HATII[4] at the University of Glasgow[5], UKOLN[6] at the

[1] Presented at the *JCDL Workshop on Digital Curation and Institutional Repositories*, 15 June 2006, Chapel Hill, North Carolina, © University of Glasgow for the Digital Curation Centre (DCC). This paper may be copied and redistributed provided it is not changed.

[2] http://www.jisc.ac.uk

[3] http://www.ed.ac.uk

[4] http://www.hatii.arts.gla.ac.uk

[5] http://www.gla.ac.uk

[6] http://www.ukoln.ac.uk

University of Bath[7] and the Council for the Central Laboratory of the Research Councils (CCLRC)[8] have collaborated to build the DCC on the international expertise and renown of the partners in research, development, service, and training delivery [11]. The DCC has four fundamental priorities: to establish a vibrant research programme, to build and foster strong community relationships, to explore innovative development activities that lead to tangible heavily used services, and to achieve a *virtuous circle* whereby every aspect of our own outputs and community input feeds into and informs our existing activities and shapes emerging ones.

Since it is anticipated that the successful development of accreditation, audit, and certification will depend on international consensus, the DCC has developed relationships with the leading audit and certification efforts in this area [10]. Much of the effort to date appears to have concentrated on defining the characteristics of a 'trusted digital repository'; considerably less effort has been committed to establishing a context in which these characteristics can be shown to be present and if they are present how their qualities can be measured and evaluated. Although here we focus on approaches to audit and certification within the archives and library community and how they might be enhanced, we have recognised elsewhere [10] that this work must not be conducted in isolation and that there is much to be gained from building on the work of other audit and certification organisations and their methods and approaches (e.g. ISACA,[9] Information Systems Audit and Control Association). As we argued earlier, '*digital curation and preservation is a risk management activity at all stages of the longevity pathway'* [10]. Many other communities have developed strategies for identifying, monitoring, and managing classes of risk that are directly relevant to our work.[10]

2. DEFINING ACTIVITIES

The generally accepted starting point for much of this work is the 2002 Research Libraries Group (RLG)[11] and Online Computer Library Centre (OCLC)[12] Working Group paper, *Trusted Digital Repositories: Attributes and Responsibilities* [9]. Subsequently, the RLG and US National Archives and Records Administration (NARA)[13] Digital Repository Certification Task Force published in late 2005 a draft *Audit Checklist for Certifying Digital Repositories* [8], comprising just under ninety criteria for determining whether a digital repository should be trusted. These criteria are organised into four categories: organisation; functions, processes and procedures; the designated community and information usability; and, technologies and technical infrastructure. The principles, terminology, and functional characteristics outlined in the Reference *Model for an Open Archival Information System* (OAIS) [7], published by the Consultative Committee for Space Data Systems (CCSDS) and subsequently galvanised as international standard ISO14721 form the bedrock on which the checklist, at least in its draft form, is built. Together, these three documents have provided a foundation for activities that are being undertaken within the Center for Research Libraries' (CRL)[14] Certification of Digital Archives[15] project with support from the Andrew W Mellon Foundation. This is currently conducting pilot audits of digital archives including the *Koninklijke Bibliotheek* (KB)[16], the Inter-University Consortium for Political and Social Research (ICPSR),[17] and Portico[18]. In addition, the CRL team will audit the distributed archiving system LOCKSS[19] ("Lots of Copies Keep Stuff Safe"). The overall aim of the CRL work is to evaluate in as formal a way as possible the audit and certification checklist proposed by the RLG-NARA Certification Task Force, and to offer some insight into the applicability of their proposed metrics. The DCC is collaborating with the CRL on the KB audit in April 2006 as a way to ensure comparability between DCC and CRL audit approaches.

A comparable German initiative the Network of Expertise in Long-term Storage of Digital Resources (*nestor*) aims to raise awareness for digital preservation issues, promote best practices, and foster the development of an associated community of expertise.[20] A *nestor* working group is exploring the development of a procedure for certification as well as a criteria catalogue for "trustworthy archives".[21] This work covers the technical, organisational, and financial characteristics of a digital repository and has conceived its own checklist for repository audit. Stefan Strathmann, Göttingen State and University Library

[7] http://www.bath.ac.uk
[8] http://www.cclrc.ac.uk
[9] http://www.isaca.org/
[10] See presentations at the ERPANET workshop on Audit and Certification in Digital Preservation held in Antwerpen from 14-16 April 2004, http://www.erpanet.org/events/2004/antwerpen/index.php
[11] http://www.rlg.org
[12] http://www.oclc.org
[13] http://www.archives.gov
[14] http://www.crl.edu
[15] http://www.crl.edu/content.asp?l1=13&l2=58&l3=142
[16] http://www.kb.nl/
[17] http://www.icpsr.umich.edu/
[18] http://www.portico.org/
[19] http://www.lockss.org/
[20] Kompetenznetzwerk Langzeitarchivierung, http://www.langzeitarchivierung.de/index.php
[21] http://nestor.cms.hu-berlin.de/tiki/tiki-index.php?page=Working+Group+on+Trusted+Repositories+Certification+%28nestor%29

(Germany) provided us with access to an early draft of the *nestor* checklist [6]. One strength of the *nestor* work is that the criteria are well founded on broad thinking in digital preservation and the criteria catalogue itself has been built on the rich literature base related to digital preservation. Recent discussions with Suzanne Dobratz indicate that *nestor* is working to develop mechanisms to assess a repositories fulfilment of the criteria.[22]

Another German example, the *Deutsche Initiative für Netzwerkinformation* (*DINI*)[23] has established a certification approach covering institutional document and publication repositories focused on examining quality of service, visibility, interoperability, and reliance on standards [3, 4]. The process starts with a repository completing an audit template. Following its submission an information specialist and a technical expert evaluate the responses and assess whether certification should be granted; this process often involves communication with the repository seeking certification and provision by them additional information. The *DINI* certificate, launched in 2003 by the Electronic Publishing working group established a minimum set of requirements for repositories and institutions which administered them, covering such issues as server policies, legal matters, and long term availability and sustainability. Although restricted to a single class repositories, *DINI* in 2006 runs the only implemented digital repository certification scheme.[24]

3. PLANNING PILOT AUDITS

To further clarify how repository audit and certification should be conducted the DCC is engaged in a series of pilot audits that will complement ongoing work in Germany and the USA. DCC audits will take place during July and August of 2006 at three organizations, including the British Atmospheric Data Centre (BADC). As a result we expect to establish an understanding of what represents an evidence base for repository audit, develop a list of the individuals who should participate in the process of gathering and presenting the evidence, assist other initiatives in defining the metrics and strategies that should be used to evaluate documentary, system and testimonial evidence, and contribute to the refining of the thinking on audit criteria and processes.

The evaluation process begins prior to the site visit, with initial research into the institutional infrastructure of the repository, the nature of its collections, and the demographics of its depositors and consumers, as an initial stage in audit planning. A pre-visit questionnaire will be sent to and returned by the target repository to provide auditors with a profile of the institution’s technical architecture, organisational structure, and financial position. It will give auditors information concerning such areas as security, performance, and management control. Supporting documentation will be requested and reviewed in advance of the on-site audit. These materials will, for instance, give auditors material to support decisions about where and how to probe during a visit, evidence to ascertain where processes, procedures, and practices are adequate. It will enable the audit team to establish an ‘Audit Plan’. This will facilitate the identification of areas where observation of practice, interviews, checking of documentation and testing (e.g. disaster recovery tests, evaluation of stratified random sample of digital objects at different points in their lifecycle) will be used. The scope and nature of these data collection instruments and the types of documentation requested will be refined as the DCC and others working in this are, such as RLG/NARA and *nestor*, develop a richer understanding of the information requirements necessary to assess repositories as an outcome of pilot audits.

Each of the three DCC pilot audits will produce three types of output, each meeting a particular need:

- First will be a ‘confidential report’ for the participating repository itself, detailing the results of the evaluation, offering suggestions for future developments that might improve their effectiveness, processes, and documentation procedures, giving guidance as to how the repository could use the audit tools to manage regular internal audits, and indicating how the repository could better prepare for future externally run audits.
- In consultation with the audited repository the DCC audit team will make publicly available a report appraising the audit approaches it employed and indicating the kinds of improvements that should be made to the process.
- Revised criteria and descriptions of the audit process will be delivered to RLG/NARA and *nestor* as the third anticipated outcome of each pilot audit.

4. WHAT IS THE EVIDENCE BASE?

Significant intellectual effort has been committed to the identification of the necessary technological, organisational, and financial characteristics repositories

[22] See the paper by Stefan Strathmann, Susanne Dorbratz, and Astrid Schoger offered at the *JCDL Workshop on Digital Curation and Institutional Repositories*, 15 June 2006, Chapel Hill, North Carolina

[23] http://www.dini.de/

[24] See for example, 'Elektronisches Formular zur Beantragung
des DINI-Zertifikats für Dokumenten- und Publikationsserver
http://www.dini.de/dini/zertifikat/fragebogen.php

must have if they are to be granted a kite-mark of trustworthiness. This is perhaps realised most notably within the *nestor* and RLG-NARA audit checklists [6, 8]. The issue of the categories of evidence necessary to facilitate audits and enable certification needs to be given adequate consideration: any tool that omits to describe the evidence which will contribute to the audit process is incomplete. If an audit checklist has aspirations of practical applicability its criteria must detail not only the expected and required standards, but also the means by which their attainment can be demonstrated and assessed. Similarly, if such tools are to promote self-assessment of a rigorous and reliable kind, and to be likely to provide a good predictor for the outcome of an independent external audit then they must be comprehensive, either independently or in combination with one or more linked resources. With no indication of its acceptable evidence base a checklist for enabling the audit and certification of a repository has mainly theoretical value. It lacks practical applicability and does not support unbiased measurement. It becomes too open to interpretation and a risk arises that it will be extrapolated to endorse even those repositories with recognisable shortcomings. Current work does not, so far, focus adequately on the evidence base; a further step of development is necessary to conceive a document that is practically useful within an audit. Efforts must probe for evidence of *concrete* processes, structures, and functionality.

In reviewing the audit tools that are being developed [6, 8] we have identified and reported a gap in the documentation requirements necessary to provide an evidence base for measuring repository compliance with the expectations for best practices as outlined in the checklists.

The types of evidence likely to be of value to an auditor will be drawn from a range of sources: information services, finance, human resources, and many others. The methods for selecting and evaluating the evidence need to be regularized. For example, presence or absence of a particular class of evidence is not necessarily a sufficient metric. Here we only seek to highlight the relevant questions and concerns, offer a series of common sense solutions, and prompt further exploration; we do not aspire to examine the issue as comprehensively as it needs to be. So we have not suggested methods for evaluating the documentary evidence. The most immediate barrier is establishing an understanding of the kinds of documentary and testimonial evidence that an auditor would seek to accumulate in considering a repository's case for certification. From this, a series of sub-questions follow:

- In what circumstances can *quantitative* metrics be established for assessing whether individual criteria have been adequately satisfied?
- How might the qualitative merits of evidence be assessed consistently by different auditors?
- What organisations and individuals should be responsible for gathering information and conducting a dialogue with repository representatives?
- What document procurement powers should be conferred to auditors?
- What assurances must be given to institutions concerned about disclosing sensitive information? (For example, will non-disclosure agreements be necessary?)
- What external benchmarking evidence might be available to auditors that could contribute to their view that an institution is compliant and certifiable?

The initial starting point though is the evidence itself; we accept the checklist format that has become *de rigueur*, but propose that at all times evidence requirements ought to be detailed inline alongside each certification criterion. Needless to say, the means of their satisfaction will be determined in part by the character and services of the particular repository undergoing audit. We favour a simple system of classification of the evidence, with conformance information categorised as *documentary evidence*, *observation of practice evidence*, or *testimonial evidence*. Here we would propose that observation can be much more than a passive activity, it might include such proactive steps as sampling, scenario sequencing, and tests.

5. DOCUMENTARY EVIDENCE

Some repository characteristics can be objectively assessed through the provision by the repository of documentary evidence and its analysis by the auditors. Insights into technical infrastructure, financial management, resource allocation, and user relationships can all be gained from the existence and analysis of a range of documentary evidence. Numerous types of documentation of value to the audit and certification process exist within repositories; for some, their presence alone will be encouraging, and in other cases their content will require scrutiny if its role in fostering organisational compliance is to be assessed. To promote an improved understanding of the kinds of documentation that might be used to support audit and certification we suggest that the following be considered as an initial list.

Repository Mission Statement: The statement of the repository's mission and if the repository is part of a larger organisation its 'spacing' within the parent organisation. This provides auditors with evidence of institutional commitment to the long-term retention and management of digital information on behalf of depositors.

Example Deposit Agreements: These agreements would enable auditors to assess the relationship between depositor and repository, the responsibilities of both parties, the level of service expected and the legal rights and obligations of the parties involved. This can help auditors to assess the suitability of repository functions and contractual controls.

Job Descriptions: As these detail the duties and responsibilities of each member of the repository staff, they give auditors evidence of the existence of capacity to deliver the kinds and levels of service outlined in the mission statement and depositor agreements. In addition they provide a mechanism for mapping between the organisational objectives and the means to deliver them.

Organisational Chart: Documents detailing the roles and responsibilities of staff and how they interrelate offer evidence of the existence of appropriate management structures and support validation of quality control mechanisms.

Staff Profiles/CVs: Overviews of experience, expertise, and qualifications of staff should be provided as these will offer an indication of the capabilities and backgrounds of individuals performing key tasks within the repository and assist in giving auditors evidence as to whether the right staff mix is available.

Annual Financial Reports: Details of income and expenditure as well as project income and expenditure provide evidence as to the financial footing and planning of the repository. This evidence should be considered for at least the three previous years. For example, the historical data will enable auditors to assess how good the repository is at predicting its future income and expenditure? This will be valuable in enabling auditors to assess repository financial risk.

Business Plan: The document detailing the financial, organisational and methodological basis for the repository, providing a justification for its existence and a plan to ensure its persistence. The Business Plan offers evidence of organisational approaches to sustainability, projected developments, and plans for exploiting emerging market opportunities.

Risk Register: How repositories approach risk management will be a central concern to auditors. They will wish to review any risk registers and access the repository's approaches to them: is the register appropriately scaled and detailed, does it indicate a proactive or reactive approach to risk, and is it likely to help the repository manage risk. A detailed list should indicate the risk, its likelihood, what actions are being taken to avoid it occurring, how the repository will respond if the risk were to occur, and what the impact of its happening would be. For example, how would the repository approach accidental disclosure of some of its holdings.

Policy Documents: Documents detailing the repository's policy in key areas, such as acquisitions, preservation strategies, guidelines for selecting and ingesting digital objects, and access and disaster recovery provide a range of insights illustrating the means by which the repository performs particular functions, provides specific services, manages its relationships with the user, and how it responds to such extrinsic factors as legislation and regulation.

Procedure Manuals: This class of documentation gives evidence of the procedures carried out by the repository in such areas as methods for validating submissions, backup, data checking, storage media change, system maintenance, and destruction of old media.

Workflow Models: These indicate the level of understanding and management of the processes applied by the repository. They also give auditors an indication of pressure points that can be tested as part of the audit visit.

Technical Architecture: Documentation of the repository's hardware and software infrastructure provide evidence to enable auditors to validate suitability of hardware and software infrastructures to support effectively the functions and services aspired to in both the mission statement and agreed in the individual depositor agreements.

Maintenance Reports: Documentation describing maintenance that has been undertaken within the system, including the application of security and functionality upgrades and the repair or replacement of corrupt or lost data objects. This enables the auditors to evaluate the effectiveness of the team and to make an assessment of the quality of service that the repository can provide.

Results of Other Audits: The results of other audits, such as Information Security, Health and Safety, and even Evidence of areas in which the repository was acknowledged by other independent auditing regimes and particular audits to have been successfully conducting its business.

Other Documentation Records: During the process of managing digital materials repositories will produce other documentary 'fingerprints'. These will need to be identified on a repository by repository basis.

Even the processes by which these documents are managed will provide auditors with valuable insights into the running of the repository. It will be useful to know how decisions are taken to draft them, how their change is reviewed, how new versions are approved, and how staff are made aware of changes to procedures and policies.

Associated with many forms of physical documentary evidence will be fears over confidentiality and privacy – every organisation has documentation that it regards as sensitive, whether for financial or business planning reasons, or those more attributable to relationships with depositors. Auditing teams need to put appropriate non-disclosure agreements in place to secure the confidence of repository representatives and that privacy and confidentiality agreements will not be breached by the audit process. The processes and practices of conducting audits are governed by a range of professional practices;

These types of documentation must be subjected to consistent and unbiased evaluation. The methods for evaluating documentation and reporting on their evaluation require further consideration. Moreover the evaluation of the submitted documentation may result in subsequent requests for additional written documentation, or the collection of evidence through observation of practice or by means of interviews.

6. OBSERVATION OF PRACTICE EVIDENCE

Witness accounts describing existing processes within the repository represent a key means of determining whether certification criteria have been met. In most cases this represents the most straightforward way in which repository workflow and good practice can be evidenced. Within the context of an institutional audit auditors themselves will expect to be exposed to the processes of ingest, archiving and dissemination. This might be most fruitfully achieved by following the passage of a single digital object throughout the full process or through the selection of different evidence points related to the passage of different objects through the process and observation of what happens at each of these points. As well as processes, technical characteristics of the repository can be assessed in this way. While observation may appear less objectively quantifiable than documentary evidence it nonetheless represents an important part of the organisational assessment and is used in other types of audit. In such areas as procedures and workflow models auditors can test how well the repository understands what it does and does what it says it does, its relationship with the users, and how it has planned to handle disasters. These observations might include walkthroughs or testing and measurement of presence of essential characteristics of digital objects against anticipated or projected characteristic survival post preservation action (e.g. after regularisation, migration, emulation). Here again our community needs to define what practices it should adopt to document these audits. Here again we can adopt practices from other communities.

7. TESTIMONIAL EVIDENCE

Interviews with stakeholders and repository staff will allow the auditor to assess internal mechanisms and organisational processes. Inevitably, documentary evidence offers incomplete insights. In most organisations there is a degree of knowledge that is locked away 'in the heads' of experienced repository staff. This in itself is a concern in terms of certification, and every repository should have mechanisms in place to mitigate risks posed by this. Interviews are an effective means of highlighting the omissions that exist within formal documentation and to validate whether the aspirations of the documents are achieved in reality.

A key step is to identify the particular individuals to be included in the interview process. Initial considerations suggest that interviews with staff fulfilling a representative sample of roles within the repository are sensible. This could stretch from Director to janitors (cleaners). For instance, a casual chat with a janitor might reveal that, although the repository's documentation states that to avoid data leakage all media from CDs to tapes are shredded or crushed before disposal this does not happen in practice. Of course, in many smaller organisations different activities that might in larger organisations be handled by different individuals might be handled by a single person. The discussion should certainly be structured in terms of roles, and not people. A series of example roles are described below:

Repository's Administrators: Those in charge of the repository's operation provide an obvious starting point, and they ought to be capable of offering an institutional overview, as well as expert insight into the repository's mission, staff appointment criteria, financial policy, and risk management strategies. While perhaps insufficiently hands-on to offer specific technical insights they will have the greatest sense of the overall workflow that is undertaken from an object's ingest through to its subsequent retrieval. This broad view ought to be exploited.

Hardware and Software Administrators: Interviews with the individual(s) responsible for the design, implementation and maintenance of repository hardware and software will assist in assessment of the appropriateness of technologies, and security, disaster recovery or integrity measures.

Ingest, Archive and Preservation and Access Officers: Those responsible for key functional units within the repository will be able to offer more in-depth insights into day-to-day operations than senior administrators. Interviews with these classes of staff should facilitate the understanding of way procedures and policies are developed and implemented.

Depositors: While there may be practical concerns associated with securing depositor testimonies, their views will contribute to establishing the repository's success in achieving the targets set within its depositor agreements. For instance, depositors will be able to verify whether they are adequately informed when processes are completed and consulted about changes to repository procedures and services. The significance of their role will be determined in many cases by the nature of the repository and its relationship with depositors.

Information Seekers: Similarly, interviews with information seekers may be difficult to set up, but they will support assessment of whether users are satisfied with the working of the repository. This would complement or provide validation of user-based evaluation work. While it is true that most validation of user evaluation can be done through assessment of protocols, processes, and outputs, there are circumstances where auditors will find it appropriate to gather their own evidence from the community.

As vital as determining the list of potential interviewees it is necessary to identify the core set of questions that will direct the dialogue and effectively marry it with the checklist being used. Current DCC research is committed to the development of a semi-structured interview template to facilitate the process of interview and personal engagement. This will be designed in away that make it extensible so that when issues arise as part of the pre-audit planning or the documentary review the template can be adjusted on an audit-by-audit basis to allow the auditors to probe for the necessary information.

8. CONCLUSION AND NEXT STEPS

Evidence will play a crucial role in the process of repository certification. Without an agreed base of evidence against which to validate the checklist criteria audits are likely to lack consistency and depend too much on judgement(s) that may prove difficult to replicate, substantiate, or validate. Unless, therefore, a checklist is associated with a defined evidence base its usefulness is diminished. Here we have considered the kinds of evidence that might provide auditors with necessary information to assess the levels of risk associated with a particular repository and to determine whether it should be certified as worthy of trust. In order to conceive an 'objective' and usable resource it is vital that any checklist offers repositories and auditors the means to understand the criteria necessary to achieve a 'worthy of trust' status in measurable (although not necessarily quantifiable) terms, and offers clear insights into how they might determine whether their own institution meets them. This approach will not only facilitate the audit process, but will also assist institutions creating new repositories in defining the processes and types of documentation they should put in place to ensure that their organisation is 'working smart' and that it is 'audit ready'. Even existing repositories may benefit from guidance on the kinds of documentation that auditors are likely to seek when assessing levels of trust. Although the community is a year or more away from spinning out audit and certification procedures, it is not too early to consider the kinds of documentation that a repository should be keeping.

While we have suggested kinds of evidence that might underpin the use of repository checklists, metrics for measuring compliance or the level[25] at which a repository meets a particular criterion require more research. As a corollary we might consider Chapin and Akridge's reflection that '[t]raditional security metrics are haphazard at best; at worst they give a false impression of security that leads to inefficient or unsafe implementation of security measures' [2]. This is a scenario that the repository community should wish to avoid. And, if we are to avoid it, we need to establish a secure evidence base and agree metrics for evaluating it.

There is a downside to considering the repository audit and certification process from the point of view of evidence—it makes it readily apparent how much effort will be involved in the audit process and how high the cost is likely to be in a way that checklists alone do not. On the other hand, by considering the evidence and underlying processes, at an early stage, repositories will be able to contain costs through adopting best practices.

Finally as a community we need consider how other audit and certification tools might be integrated with our emerging checklists or tailored to meet our needs. As Hans Hofman, of the Dutch National Archives, has observed on many occasions any new methods need to be placed in the

[25] It might even be worth asking about 'the way' in which checklist criteria are satisfied.

larger audit context which includes such approaches as the COSO framework for audit[26], COBIT framework (Control Objectives for Information and Related Technologies)[27], ITIL (IT Infrastructure Library) service management[28], ISO 9000 family of quality management and assurance standards[29], and ISO 17799 for information security[30]. The digital repository building and management community, such as libraries and archives, does not appear so far to have paid sufficient attention to these other strands of activity and tools. They do have much to offer us and, we believe, we have much to learn from them. This work should be undertaken alongside further refinement of evidence requirements and development of metrics for assessing and measuring checklist compliance.

9. CONTRIBUTORS

Both authors participated in the definition of this work, analysis and synthesis, and drafting of the manuscript. They agreed the final version of the manuscript.

10. CONFLICTS OF INTEREST

We declare that we have no conflict of interest.

11. ACKNOWLEDGMENTS

The Digital Curation Centre is supported by a grant from the UK Joint Information Systems Committee (JISC) and the UK e-Science Core Programme of the Engineering and Physical Sciences Research Council (EPSRC). We are grateful to Niklaus Bütikofer, formerly of the Swiss Federal Archives, who is working with us to define the DCC's audit and certification working practices, for discussions. We wish to thank Robin Dale of RLG and David Giaretta of the DCC and Principal Investigator in CASPAR for discussion and providing us with early access to the RLG/NARA Checklist [8]. We are grateful to Stefan Strathmann, Göttingen State and University Library (Germany) kindly supplied us with an early draft of the *nestor* audit and certification guidelines [6]. Hans Hofman of the Dutch National Archives has over the past couple of years shared crucial thinking with us in this area and we are beginning to work with him in the context of the European Commission funded Sixth Framework project, DigitalPreservationEurope[31] (DPE) to take repository audit and certification initiatives forward in the European context. Helen Hockx-yu (JISC) and Helen Tibbo of the University of North Carolina kindly offered valued comments of the penultimate draft of the paper. Some DPE partners are also partners in DCC and *nestor*.

12. WEB SITE CITATIONS

All citations of websites were validated on 24 May 2006.

13. REFERENCES

[1] S. Anderson and R. Heery, 2005, *Digital Repositories Review*. http://www.jisc.ac.uk/uploaded_documents/digital-repositories-review-2005.pdf.

[2] D. A. Chapin, and S. Akridge, 2005, 'How Can Security Be Measured?', Information Systems Control Journal, volume 2 2005, http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=24174&TEMPLATE=/ContentManagement/ContentDisplay.cfm

[3] DINI Working Group "Electronic Publishing, 2003, DINI-Certificate, Document and Publication Repositories http://www.dini.de/zertifikat/dini_certificate.pdf

[4] DINI Arbeitsgruppe 'Elektronisches Publizieren', 2003, DINI Zertifikat, Dokumenten- und Publikationsserver, http://www.dini.de/dini/zertifikat/zertifikat.php

[5] ERPANET, 2004, 'The Role of Audit and Certification in Digital Preservation', Stadsarchief Antwerpen, Belgium 14-16 April 2004 (2004)

[6] Die nestor-Arbeitsgruppe 'Vertrauenswürdige Archive – Zertifizierung', 2006, Kriterienkatalog vertrauenswürdige digitale Langzeitarchive--ENTWURF, (March 2006), Berlin and München. (privately circulated).

[7] *Reference Model for an Open Archival Information System (OAIS) – ISO 14721*, 2002). http://www.ccsds.org/documents/650x0b1.pdf

[8] RLG/NARA Task Force on Digital Repository Certification, 2005, *Audit Checklist for Certifying*

[26] Committee of Sponsoring Organizations of the Treadway Commission (COSO), http://www.coso.org/publications.htm

[27] www.isaca.org/cobit/ COBIT a reference framework for measuring performance, ascertaining success factors and using maturity models for benchmarking. It was released by the IT Governance Institute (ITGI).

[28] ITIL, created by the UK's Office of Government Commerce, is a library of best practice processes for IT service management. (see ISO/IEC 20000) http://www.itgovernance.co.uk/page.itil

[29] See for instance, http://www.iso.org/iso/en/iso9000-14000/understand/selection_use/selection_use.html

[30] ISO/IEC 17799:2005: Information technology - Security techniques - Code of practice for information security management, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3=

[31] http://www.digitalpreservationeurope.eu

Digital Repositories, http://www.rlg.org/en/pdfs/rlgnara-repositorieschecklist.pdf.

[9] RLG/OCLC Working Group on Digital Archive Attributes, 2002, *Trusted Digital Repositories: Attributes and Responsibilities*, http://www.rlg.org/longterm/repositories.pdf

[10] S. Ross and A. McHugh, 2005, ‘Audit and Certification: Creating a Mandate for the Digital Curation Centre’, Diginews, Vol 9 no 5, ISSN 1093-5371, http://www.rlg.org/en/page.php?Page_ID=20793#article1

[11] 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