



ERPANET@SAA2004:
Certification and Audit
SA Pre-Conference Workshop
30 August 2004, Glasgow

Seamus Ross, ERPANET



Presentation based on
ERPANET's Antwerp Workshop
See Antwerp presentations at:

<http://www.erpanet.org>

Repositories

- Archives must maintain trust over time
- Retrospective auditing of the chain of processing (e.g. management) essential
- Digital materials require archives be more transparent, public, and open

The Problem

- 'Is it safe' *Marathon Man* (1976)
- How do we know that our data are secure
- Trust
 - How is it established?
 - How is it maintained?
 - How is it secured?
 - What happens when it is lost?
 - How can it be verified?



The Call for Certification

“A critical component of the 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 for certification of digital archives is needed to create an overall climate of trust about the prospects of preserving digital information.”

Task Force on Archiving of Digital Information,
Preserving Digital Information, 1996.



Why and Who needs Certification

- Potential depositors
- Future Users
 - Persons
 - Machines (use might depend upon level of certification)
- Managing organisations

Who will seek certification?

- Cost of certification will influence this
- Relevancy to mission, goals, remit
- Organisations likely to seek certification:
 - National libraries, archives, data centers with legal remit/mandate
 - Large research libraries
 - Consortial/federated repositories
 - Third party service providers (e.g. commercial repositories and archives)

Certification will not be required by every repository?
Or will it?

RLG/NARA on Trust

- “The goal of this project is to design a digital archiving service that is capable of reliably storing, migrating, and providing access to digital collections.”
- “The challenge is to produce certification requirements, delineate a process for certifications, and identify a certifying body (or bodies) that can implement the process.”
- From: www.rlg.org/en/page.php?Page_ID=580

Trusted Repositories

- What is one?
- RLG/OCLC Proposal
 - need a programme for certifying trusted repositories
 - checklist of concept and key elements needed
- Depends on definable, certified and auditable practices
- What would certification guarantee and how would it be revoked and with what implications
- Expectation of *Open Archival Information System Reference Model (ISO 14721:2002)*

Aspects need certification

- People
 - through developing competencies
- data
 - Quality management, policy, validation
- processes
 - OAIS model, ingest, storage, IPR, organisational practices
- managing organisations
 - audit of approaches organisations take to data management

Certification

- Statement of attributes to be measured
- Policies and assumptions (e.g. practices, environment and security)
- Procedures against standards
- Relationship with depositors
- What processes are in place to manage fidelity checks for ingest
- What metadata processes are in place
- What user needs evaluation work is carried out



Trusted Digital Repositories: Attributes and Responsibilities (2002)

- Defined trusted digital repository
- Listed attributes of a trusted digital repository
 - Compliance with OAIS
 - Administrative responsibility
 - Organizational viability
 - Financial sustainability
 - Technological and procedural suitability
 - System security
 - Procedural accountability
- Recommendation: Develop a process for the certification of digital repositories.



RLG & NARA: International Workgroup

- National Libraries
- National Archives
- Universities
- Government space data agencies
- University/Consortial data center
- Collaborative organizations
- Third party service provider
- Internet Archive

Objective: Create a standard certification process or a framework that can be implemented across domains or types of digital repositories

http://www.rlg.org/en/page.php?Page_ID=367

RLG/NARA Workgroup Tasks

- Identify certifiable elements (attributes, processes, functions, activities) of a digital repository or types of repositories
- Define a standard certification process or a framework that can be implemented across domains or types of digital repositories.
- Develop certification plan(s)
- Define the conditions for revocation of certification and suggest appropriate action plans for endangered digital information

Certification Framework

- Levels of certification?
- Self certification?
- Bit preservation?
- Information preservation?
- Certifiable elements? Are those suggested in the original report the correct ones?
- Certifying body/organization?
- Duration of certification?
- Consequences of revocation?

Rumours indicate thinking towards

- Toolkit
 - Self certification
 - “Independently administered” certification
- Certification
 - Baseline requirements
 - Additional levels or “modules” likely



Certifiable Elements

(Dale Rome03, Giaretta Antwerp 04)

- Minimum Attributes (Metrics)
 - *Trusted Digital Repositories*
 - Compliance with OAIS
 - Administrative responsibility
 - Organizational viability
 - Financial sustainability
 - Transparency, etc.
 - Technological and procedural suitability
 - Existing “computer center” practices of requirements
 - System security
 - Back-up, recovery, etc.
 - Procedural accountability
 - Policies, practices documented, etc.

Certifiable Elements

(Dale Rome03, Giaretta Antwerp 04)

- Minimum attributes (continued)
 - Minimum preservation level
 - Storing objects with metadata
 - Retrieval
 - Rendering?
- Curatorial aspects
- Audit aspects
- “Customer perspective”
 - Levels of service
- What other attributes are there?

Audit / Review

- What information does an audit need?
 - Policies defined by the archives
 - Inner workings of the archives (workflows)
 - Chain of custody of an archivalia (enactment and results of workflows)
- Who will perform the audits?
- Audit information must become part of the archive's holdings
 - Important for the understanding of the context of the other holdings for future users

Categories of Audit

- Internal audit
 - Self assessment
 - Internal Audit Service
- External audit
 - Financial auditing
 - Operational auditing
 - IT/EDP systems and services audit

Methods

- Say what you claim to do
- Demonstrate that you can do it
- Demonstrate that you do do it
- Currently working through peer-review exercises
- Requirements in each section
- Certification metrics
- Statements & documents



Example requirement (Antwerp: Ashley 04)

- 2.7: “The repository has written agreements with depositors that address all appropriate aspects of acquisition, maintenance, access and withdrawal”
- In context of this requirement a Trusted Repository must:
 - demonstrate that such agreements exist
 - demonstrate they are adequate
 - demonstrate they are adhered to

How does audit and certification happen

- Is peer review acceptable ? Achievable ?
- What will repositories pay for certification?
- How detailed/rigorous does an pre-certification audit need to be?
- What is their incentive to pay?
- Who will conduct the audit?
- How will independence be ensured?
- DCC in the UK will provide audit and certification in HE's and FE's

The role of the collecting policy

- Clearly relevant to research libraries
 - but what about other sorts of repository ?
- Service providers work in a different organisational framework
- Collection policy may not control quality of what is preserved
- But we can audit how it is preserved

Possible Certification Process/Stages

- Self-certification – check list (internal)
- Peer-group (maybe mostly applicable to Libraries)
- Independent Certification – externally managed

RLG/NARA only one Approach

- There are other developed models that should be given consideration as the foundation for repository certification.
- COSO
 - USA, Internal Control Integrated Framework, 1992
 - business ethics, effective internal control, corporate governance
- COBIT
 - Governance, control and audit for IT and related technology, 1996
 - IT-controls support the COSO-framework

COSO

Committee of Sponsoring Organisations
of the Treadway Commission (fraudulent financial reporting)

Internal Control Integrated Framework

1. Control environment (company level)
2. Risk assessment (achieve objectives)
3. Control activities (policies, procedures, practices, general & application controls)
4. Information and communication (at all levels)
5. Monitoring of the internal control (oversight)

CobiT

- Planning and Organisation
 - strategy, quality, human resources
- Acquisition and Implementation
 - systems development and installing
- Delivery and Support
 - service levels, operations, security
- Monitoring
 - internal control, assurance, audit

What could it Audit

- Business processes
 - input, througput, output, outcome
- People
- Application systems
- Technology
- Facilities
- Data

Special Cases: Distributed repositories

- Where a community adopts a system such as LOCKSS
- Well-controlled communities may be amenable to audit
- But responsibilities may still be unclear
- These models design institutional failure away
- Reliable - but not auditable?

Outstanding Challenges

- What will be the object of certification, the repository (is this defined?), the organisation behind it, the system or the whole?
- Why is certification necessary or will regular audits be sufficient?
- Will certification increase validity of and trust in services provided by digital repositories?
- Will it give external users a better feeling about the trustworthiness than if only regular (external) audits were carried out?



Outstanding Challenges

- Institutions as libraries and archives never are certified for the paper publications and records they preserve and provide access to. Why is it necessary to have audits and even certification now for digital objects? Have they become less reliable? What are the expectations of the different stakeholders (e.g. publishers, the public, records creators, government, users)?
- Who are the likely consumers of audit or certification – who wants it to happen?
- What difference will the existence of an audit or certification process make to the market, or to the activities of stakeholders in it?

Audit Challenges

- What do we want to achieve or pursue with audit?
- What should be audited? Under what circumstances?
- Who should do the audits (e.g. specialised bodies or not) and what are the requirements for auditing organisations?
- What framework(s) do we need in relation to the different business contexts to conduct an audit?
- Will the framework(s) allow different levels of compliance?
- What is necessary to conduct a proper audit?
- What steps should the audit process encompass?
- Should an audit be followed by certification?



- Goals, strategy and policy
- Laws and regulations
- Standards and control models
- Commitment on top level

Plan

Do

- Needs
- Responsibilities
- Projects
- Communication
- Meetings
- Organisation
- Quality
- Security

Management cycle

Correct/ Adapt

- Monitor, evaluate, learn
- New standards?
- Adapt policy

Check

- Measure
- Alignment
- Compliance
- Assessment
- Audit/assurance

Can your organisation anticipate

- Define objectives and aims of your repository and those of the services it will provide
- Develop and monitor the application of policies and procedures
- Define senior management steering roles and responsibilities in relationship to repositories
- Ensure that all services, technologies (hardware and software), exceptions
- Develop and maintain risk registers
- Status reports and minutes of meetings
- Define, implement, and monitor disaster recovery services