Managing Digital Content over Time:
Protecting Our Resources

May 2013
Chris L. Erickson
Managing Content Over Time

- Identify
- Select
- Store
- Protect
- Manage

Provide
Why **identify** content?

- Preservation requires a **commitment** of resources
- Identifying content is a first step to making **informed** decisions
- Effective planning is based on knowing what **needs** to be preserved now and in the future
- **Not all** of our digital content will be preserved

A detailed inventory is the best way to identify content
Why select content to preserve?

- Storage may be cheap, management is not... especially over time
- What can we reasonably do
- What your stake holders need
- Matching mission to content
Archival Storage

Computer Backups are not preservation

• Backups:
  – Restoring files in case of a failure
  – Temporary

• Preservation:
  – Care for individual files over time
  – Spans generations of technology
  – Not compressed; not encrypted
  – Stored with information about the objects
  – Software and hardware independent
What are we storing?

Digital content: files + metadata = object

• May include any type of content
  – e.g., images, text, sound, video, maps

• Requires some identification and description
  – Captured as metadata
Storage Considerations

Multiple, geographically distributed copies

• Minimum: two copies in two locations
• Hosted services / Storage partners
• How to decide?
  • Cost
  • Expertise
  • Services
• Online, near-line, offline
Storage Partners

• Multiple, geographically distributed
• Trusted Storage Partners
• Hosted services, e.g.

Digital Preservation Outreach and Education (DPOE)
Balanced Management

An effective approach will address:

• Organizational requirements and objectives
• Technological opportunities and change
• Resources – funding, staff, equipment, etc.
What are we **Protecting** content from?
Change or Loss
Accidental and intentional
Obsolescence

Evolving Technology
Inappropriate access
Confidential or restricted data

ATTENTION AUX PICKPOCKETS
Non-compliance

Standards and requirements
Disasters

Emergencies of all kinds
Everyday Protection

- Where is your content located?
- Who has access to it?
- Who can change the content?
Risk Management

Steps to protect your content:
• Identify and define possible risks to the data
• Assess potential damage / impact
• Detect errors, problems, damage
• Develop appropriate, feasible plans
• Respond to risks, threats - implement plans
What is Long-term Access?

Digital Preservation

• makes long-term access possible...
• provides a path from one generation of technology to the next
Questions?

Chris Erickson
cle@byu.edu
Preservation Metadata

All the information needed to manage, find and use digital content over time

Metadata enables long-term preservation

**Content**: preserve the substance
**Fixity**: demonstrate content is unchanged
**Reference**: identifies this content and no other
**Provenance**: trace to its origin (or to deposit)
**Context**: preserve linkages with other objects

Outcomes

Digital preservation requires an organization to:

• Develop a storage management policy  
  – E.g., number of copies, locations, fixity means
• Specify storage service or partner agreements
• Monitor copies of content for errors/change
• Plan for media replacement
Importance of Standards

Open Archival Information Standard

Figure 4-1: OAIS Functional Entities
ISO Standards

Certification (ISO 16363)

OAIS (ISO 14721) -> TRAC

Requirements For Bodies Providing Audit And Certification (ISO 16919)

Audit and Certification of Trustworthy Digital Repositories (ISO 16363)

- Audit by external auditors
- Monitored self-audit using ISO 16363 (or DIN1664 in Germany)
- Basic Certification
- Data Seal of Approval
- Extended Certification
- Formal Certification

There is a hierarchy of ISO standards concerned with good auditing. ISO 16919 is positioned within this hierarchy in order to ensure that these good practices can be applied to the evaluation of the trustworthiness of digital repositories using ISO 16363. It covers principles needed to inspire confidence that third party certification of the management of the digital repository has been performed with impartiality, competence, responsibility, openness, confidentiality, and responsiveness to complaints.

Metrics concerning:
- Organizational Infrastructure
  - e.g. The repository shall have a documented history of the changes to its operations, processes, software, and hardware.
- Digital Object Management
  - e.g. The repository shall have access to necessary tools and resources to provide authoritative Representation Information for all of the digital objects it contains.
- Infrastructure and Security Risk Management
  - e.g. The repository shall have procedures in place to evaluate when changes are needed to CURRENT software.


Standards will be available free from http://www.ccsei.org

EUROPEAN FRAMEWORK FOR AUDIT AND CERTIFICATION OF DIGITAL REPOSITORIES to be promoted by the EU

Digital Preservation Outreach and Education (DPOE)