Policy Recommendations for Institutions to Serve as Trustworthy Stewards of Research Data

Robert R. Downs[1], David Giaretta[2], and J. Steven Hughes[3]

[1]Center for International Earth Science Information Network (CIESIN), Columbia University

[2]Alliance for Permanent Access

[3]NASA Jet Propulsion Laboratory

Research Data Access and Preservation Summit
San Diego, California, 26-28 March, 2014

Developing and Implementing Institutional Policies on Research Data: Ownership, Preservation, and Compliance
Wednesday, March 26, 2014

The Open Archival Information System (**OAIS**) Reference Model, published as ISO 14721, has been adopted as the "de facto" standard for systems that preserve data. ISO 16363, the standard for **Audit And Certification Of Trustworthy Digital Repositories**, is based on ISO 14721 and contains the criteria for auditing various kinds of repositories in terms of their potential to provide trustworthy services for **data management and preservation**. Institutions that manage repositories for research data need to attain compliance with ISO 16363 if they plan to serve as **trustworthy digital repositories**. As an initial step, institutions that operate repositories for managing and preserving research data should create and follow policies to address the ISO 16363 requirements.

Recommendations are offered for **establishing and implementing policies** within institutions that plan to serve as **trustworthy repositories of research data holdings**.

ISO 16363 Requirements Categories

Organizational Infrastructure	Digital Object Management	Infrastructure and Security Risk Management
• Governance and Organizational Viability • Organizational Structure and Staffing • Procedural Accountability and Preservation Policy Framework • Financial Sustainability • Contracts, Licenses, and Liabilities	• Ingest: Acquisition of Content • Ingest: Creation of the AIP • Preservation Planning • AIP Preservation • Information Management • Access Management	• Technical Infrastructure Risk Management • Security Risk Management

Source: Consultative Committee for Space Data Systems. 2011. Audit and Certification of Trustworthy Digital Repositories. Recommended Practice. CCSDS 652.0-M-1. Magenta Book. September, 2011. http://public.ccsds.org/publications/archive/652x0m1.pdf

Organizational Structure: Relevant Policies

ISO 16363 Requirements

- Governance and Organizational Viability
- Organizational Structure and Staffing
- Procedural Accountability and Preservation Policy Framework
- Financial Sustainability
- Contracts, Licenses, and Liabilities

Relevant Policies

- Sustainability Policy
- Professional Development Policy
- Records Management Policy
- Fiscal Policy
- Data Policy
- Privacy Policy
- Content Dissemination Policy
- Linking Policy

Digital Object Management: Relevant Policies

ISO Requirements

- Ingest: Acquisition of Content
- Ingest: Creation of the AIP
- Preservation Planning
- AIP Preservation
- Information Management
- Access Management

Relevant Policies

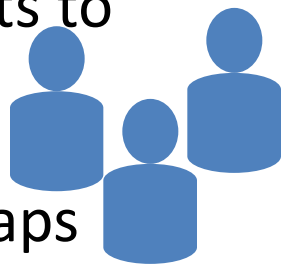
- Data Acquisitions Policy
- Collection Management Policy
- Data Management Policy
- Digital object content policy
- Preservation of Digital Resources Policy
- Data and Information Management Policy
- Data Policy
- Policy for Identifying Versions of Archived and Disseminated Resources

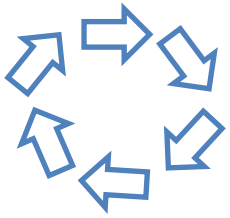
Infrastructure and Security Risk Management : Relevant Policies

ISO 16363 Requirements	Relevant Policies
• Technical Infrastructure Risk Management • Security Risk Management	• Risk Management Policy • Security Policy

Establishing Policies for Trustworthy Data Stewardship

- Identify gaps for achieving compliance with ISO 16363 requirements throughout the data lifecycle
  - Determine which policies to create, based on "Examples of documents the repository can use to demonstrate that it is meeting this requirement"
- Establish team or hire consultants to identify elements to be covered by each policy
  - Team or consultants should possess relevant experience
- Draft policies to address the ISO 16363 compliance gaps
  - Identify and review similar policies from other organizations
- Review, refine, and approve policies to ensure attainment of trustworthy stewardship throughout data lifecycle
  - Policies must be approved by organizational leaders



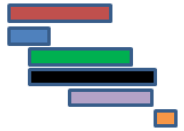
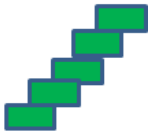
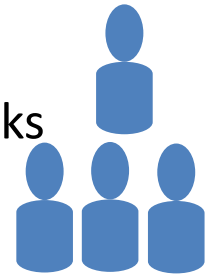


Example Language for Policies

- Data Policy:
  - "unrestricted access and use of data without charge“; "are freely distributable and re-distributable ... unless otherwise specified in the documentation“; "rights and permissions associated with each particular data set are specified in the documentation of the data“ (http://ciesin.columbia.edu/documents/CIESINDataPolicy.pdf)
- Data and Information Management Policy:
  - "will maintain records on the status of all data or information created“; "appropriate permissions will be obtained from external sources“; "managed in such a manner to protect privacy and confidentiality of individual-level data as appropriate“ (http://ciesin.columbia.edu/documents/CIESINDataInfoMgtPolicy.pdf)
- Policy for Preservation of Digital Resources
  - "identify and employ recognized standards and maintain currency of hardware, software, metadata and data formats“; "identify research initiatives and results that would improve digital preservation planning and practices“; "obtain training on current practices for archiving, managing, and preserving digital resources“ http://ciesin.columbia.edu/documents/CIESINpreservationpolicy.pdf

Implementing Data Stewardship Policies

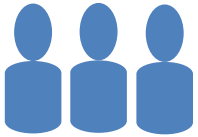
- Specify Workflow
  - Define and establish the order (sequential and parallel) of tasks that must be completed to implement the established policies
- Develop Procedures
  - Write detailed descriptions of steps necessary for completing each task to ensure compliance with policies
- Conduct Training
  - Provide instruction for individuals responsible for completion of tasks that is consistent with policies
- Adopt Practices
  - Staff perform tasks in accordance with the policies, procedures, and training.
- Assess Implementation
  - Verify that work is performed in a manner that is consistent with policies

Audits Help to Ensure Compliance

- Internal Audits: Primarily Subjective
  - Desk audits (independent criteria: e.g. Data Seal of Approval, NESTOR, ISO 16363)
  - Self-Assessments: Preparation for audits
    - Conducted by management, committees, individuals
- External Audits: Independent Evaluation
  - Independent Auditors, Professional associations
  - Accreditation Boards (ISO 16919: Requirements for Bodies Providing Audit and Certification of Candidate Trustworthy Digital Repositories)



References and Resources

- Consultative Committee for Space Data Systems. 2011. Audit and Certification of Trustworthy Digital Repositories. Recommendation for Space Data System Practices. Recommended Practice. CCSDS 652.0-M-1. Magenta Book. September, 2011. [Published as ISO 16363:2012] http://public.ccsds.org/publications/archive/652x0m1.pdf
- Consultative Committee for Space Data Systems. 2012. Reference Model for an Open Archival Information System (OAIS). Recommendation for Space Data System Practices. Recommended Practice CCSDS 650.0-M-2. Magenta Book. June 2012. [Published as ISO 14721:2012] http://public.ccsds.org/publications/archive/650x0m2.pdf
- Holdren, J.P. 2013. Increasing Access to the Results of Federally Funded Scientific Research. February 22, 2013. http://www.whitehouse.gov/sites/default/files/microsites/ostp/ostp_public_access_memo_2013.pdf
- Primary Trustworthy Digital Repository Authorization Body. 2013. Preparing for an ISO 16363 Audit. http://www.iso16363.org/preparing-for-an-audit/


REPOSITORIES
TRUSTWORTHY
INSTITUTIONS
ISO
data
POLICIES
RESEARCH
RECOMMENDATIONS
preserve
STANDARD
digital
AUDITING
serve
STEWARDS
Archival
adopted
Certification
OAIS
PUBLISHED
OPEN
REFERENCE
CRITERIA
CONTAINS
systems
Model
PLAN
requirements
ESTABLISHING
repositories
OFFERED
BASED
INITIAL
HOLDINGS
KINDS
NEED
VARIOUS
implementing
operate
STEP
MANAGEMENT
ADDRESS
COMPLIANCE
AUDITING
preserve
TRUSTWORTHY
INSTITUTIONS
potential
auditing
TERMS
FACTO
PROVIDE
RESEARCH
ADOPTED
services
criteria
IMPLEMENTING
policies
FOLLOW
create
Stewards
CONTAINS
ATTAIN
SERVE
RECOMMENDATIONS
digital
SYSTEMS
STANDARD