

**From production to preservation to access to use:  
OAIS, TDR, and the FDLP**  
Federal Depository Library Conference, October 2011  
Presentation Handout  
James A. Jacobs  
Data Services Librarian emeritus, University of California San Diego

**OAIS**

- ORIGINAL (free): Consultative Committee for Space Data Systems. *Reference Model for an Open Archival Information System*. (OAIS) CCSDS 650.0-B-1. "BLUE BOOK" (CCSDS Secretariat, January 2002). [148pp, free]  
<http://public.ccsds.org/publications/archive/650x0b1.pdf>.
- ISO STANDARD (fee): International Organization for Standardization. *Open archival information system -- Reference model* (ISO 14721:2003). [141 pp, 224 Swiss Francs]  
[http://www.iso.org/iso/catalogue\\_detail.htm?csnumber=24683](http://www.iso.org/iso/catalogue_detail.htm?csnumber=24683)
- NEW DRAFT (free): Consultative Committee for Space Data Systems. *Reference Model for an Open Archival Information System*. (OAIS) Draft Recommended Standard CCSDS 650.0-P-1.1 (PINK BOOK) Issue 1.1, August 2009 [131 pp, free]  
<http://public.ccsds.org/sites/cwe/rids/Lists/CCSDS%206500P11/Attachments/650x0p11.pdf>
- NEW DRAFT ISO STANDARD (fee): International Organization for Standardization. *Open archival information system -- Reference model* (ISO/DIS 14721). [141 pp, 98 Swiss Francs]  
[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_ics/catalogue\\_detail\\_ics.htm?csnumber=57284](http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=57284)

**TRAC / TDR**

- Trusted Digital Repositories: Attributes and Responsibilities*. An RLG-OCLC Report. Mountain View, CA: RLG, May 2002.  
<http://www.oclc.org/programs/ourwork/past/trustedrep/repositories.pdf>
- TRAC: Center for Research Libraries and OCLC. *Trustworthy Repository Audit and Certification: Criteria and Checklist*, Version 1, (2007). [94pp, free]  
[http://www.crl.edu/sites/default/files/attachments/pages/trac\\_0.pdf](http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf)
- TDR: Consultative Committee for Space Data Systems, *Audit And Certification Of Trustworthy Digital Repositories*, "Red Book," Issue 1, DRAFT RECOMMENDED PRACTICE, CCSDS 652.0-R-1 (Washington D.C.: CCSDS, October 2009). [78pp, free]  
<http://public.ccsds.org/sites/cwe/rids/Lists/CCSDS%206520R1/Attachments/652x0r1.pdf>
- DRAFT ISO STANDARD (fee): *Audit and certification of trustworthy digital repositories*. ISO/DIS 16363. [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=56510](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56510)

## Other Related Standards

*Data Seal of Approval* (n.d.) Data Seal of Approval: Quality Guidelines for Digital Research Data, online at: <http://www.datasealofapproval.org/>

*DRAMBORA*: The Digital Repository Audit Method Based on Risk Assessment. Digital Curation Centre and DigitalPreservationEurope (DPE). <http://www.repositoryaudit.eu/>

NESTOR. *Catalogue of Criteria for Trusted Digital Repositories*. Network of Expertise in long-term STORage. nestor Working Group on Trusted Repositories Certification:, Version 1 (draft for public comment), June 2006, Frankfurt am Main. [http://files.d-nb.de/nestor/materialien/nestor\\_mat\\_08-eng.pdf](http://files.d-nb.de/nestor/materialien/nestor_mat_08-eng.pdf)

*PAIMAS*: [ISO 20652:2006] *Producer-Archive Interface Methodology Abstract Standard*. CCSDS 651.0-M-1. MAGENTA BOOK. May 2004. <http://public.ccsds.org/publications/archive/651x0m1.pdf>

*PREMIS*: PREMIS Data Dictionary for Preservation Metadata. Version 2.0, PREMIS Editorial Committee, March 2008; <http://www.loc.gov/standards/premis/v2/premis-2-0.pdf>

ISO 9000 family of standards. “An international consensus on good quality management practices.”

ISO 15489-1:2001 and ISO 15489-2:2001. Records management.

ISO 15889:2003 Space data and information transfer systems—Data Description Language—EAST Specification;

ISO 21961:2003 Space data and information transfer systems—Data Entity Dictionary Specification Language (DEDSL)—Abstract syntax;

ISO 23081-1:2006, ISO/TS 23081-2:2009 Metadata for records

ISO/IEC 27002:2005. Code of practice for information security management.

## Other Material

Beedham, Hilary, Julie Missen, Matt Palmer, and Raivo Ruusalepp. *Assessment Of UKDA And TNA Compliance With OAIS And METS Standards*, "Appendix 5: A Set Of Questions For OAIS Compliance Self-Testing." (Wivenhoe Park, Colchester, Essex: UK Data Archive, 2005), p. 111 <http://www.esds.ac.uk/news/publications/oaismets.pdf>.

This is a 3-page list of questions prompted by OAIS. They are generic enough to be relevant to most OAIS archives.

Hernon, Peter 'Information Life Cycle: Its Place in the Management of U.S. Government Information Resources', *Government Information Quarterly*, 11 (1994), 143-170 doi:[10.1016/0740-624X\(94\)90002-7](https://doi.org/10.1016/0740-624X(94)90002-7).

Jacobs. James A., "Privatization of GPO, Defunding of FDsys, and the Future of the FDLP." *FreeGovInfo*. (Aug. 11, 2011) <http://freegovinfo.info/node/3416>

NLM Digital Repository Working Group. *Requirements for an NLM Digital Repository: Report and Recommendations*. (2007). <http://www.nlm.nih.gov/digitalrepository/NLM-DigRep-Report-rev032007.pdf>

Ross, Seamus, and Andrew McHugh, 'The Role of Evidence in Establishing Trust in Repositories', *D-Lib Magazine*, 12 (2006) doi:[10.1045/july2006-ross](https://doi.org/10.1045/july2006-ross).

As you think about what documents and other kinds of evidence you might use to demonstrate OAIS/TRAC compliance, this piece should be of help. The authors "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."

Steinhart, Gail, Dianne Dietrich, and Ann Green, 'Establishing Trust in a Chain of Preservation: The TRAC Checklist Applied to a Data Staging Repository (DataStaR)', *D-Lib Magazine*, 15 (2009) <http://www.dlib.org/dlib/september09/steinhart/09steinhart.html>.  
An example of a "staging repository" model.

Strodl, Stephan, Christoph Becker, Robert Neumayer, and Andreas Rauber, "How to Choose a Digital Preservation Strategy," in *Proceedings of the 2007 Conference on Digital Libraries - JCDL '07* (presented at the the 2007 conference, Vancouver, BC, Canada, 2007), p. 29 doi:[10.1145/1255175.1255181](https://doi.org/10.1145/1255175.1255181)

Although this paper focuses on one specific strategy for preservation (the PLANETS Preservation Planning approach), it nevertheless demonstrates how a one organization made decisions on how to implement OAIS to preserve digital objects for a given purpose.

U.S. Government Printing Office. Library Services and Content Management Business Unit and Federal Digital System (FDsys) Program Management Office. *Information Technology Glossary*. ("GPO Glossary v1.0"). (Last updated: 07-03-2008).  
[http://www.fdlp.gov/home/repository/doc\\_download/530-information-technology-glossary](http://www.fdlp.gov/home/repository/doc_download/530-information-technology-glossary)

U.S. Superintendent of Documents. *SOD 301, Dissemination/Distribution Policy for the Federal Depository Library Program*. Sept. 28, 2006.  
[http://www.fdlp.gov/home/repository/doc\\_download/567-disseminationdistribution-policy-for-the-federal-depository-library-program-sod-301](http://www.fdlp.gov/home/repository/doc_download/567-disseminationdistribution-policy-for-the-federal-depository-library-program-sod-301)

## OAIS Conformance

### 1.4 CONFORMANCE

A conforming OAIS archive implementation shall support the model of information described in 2.2. The OAIS Reference Model does not define or require any particular method of implementation of these concepts.

A conforming OAIS archive shall fulfill the responsibilities listed in 3.1.

### 3.1 MANDATORY RESPONSIBILITIES

This subsection establishes mandatory responsibilities that an organization must discharge in order to operate an OAIS archive.

The OAIS must:

- Negotiate for and accept appropriate information from information Producers.
- Obtain sufficient control of the information provided to the level needed to ensure Long-Term Preservation.
- Determine, either by itself or in conjunction with other parties, which communities should become the Designated Community and, therefore, should be able to understand the information provided.
- Ensure that the information to be preserved is **Independently Understandable** to the Designated Community. In other words, the community should be able to understand the information without needing the assistance of the experts who produced the information.
- Follow documented policies and procedures which ensure that the information is preserved against all reasonable contingencies, and which enable the information to be disseminated as authenticated copies of the original, or as traceable to the original.
- Make the preserved information available to the Designated Community.

## Sample TDR Metrics

### 3.4 FINANCIAL SUSTAINABILITY

**3.4.1 The repository shall have short- and long-term business planning processes in place to sustain the repository over time.**

#### **Supporting Text**

This is necessary in order to ensure the viability of the repository over the period of time it has promised to provide access to its contents for its Designated Community.

#### **Examples of Ways the Repository Can Demonstrate It Is Meeting This Requirement**

Up-to-date, multi-year strategic, operating and/or business plans; audited annual financial statements; financial forecasts with multiple budget scenarios; contingency plans; market analysis.

#### **Discussion**

An annual business planning process is commonly accepted as the standard for most organizations.

**3.1.2.1 The repository shall have an appropriate, formal succession plan, contingency plans, and/or escrow arrangements in place in case the repository ceases to operate or the governing or funding institution substantially changes its scope.**

#### **Supporting Text**

This is necessary in order to preserve the information content entrusted to the repository by handing it on to another custodian in the case that the repository ceases to operate.

#### **Examples of Ways the Repository Can Demonstrate It Is Meeting This Requirement**

Written and credible succession and contingency plan(s); explicit and specific statement documenting the intent to ensure continuity of the repository, and the steps taken and to be taken to ensure continuity; escrow of critical code, software, and metadata sufficient to enable reconstitution of the repository and its content in the event of repository failure; escrow and/or reserve funds set aside for contingencies; explicit agreements with successor organizations documenting the measures to be taken to ensure the complete and formal transfer of responsibility for the repository's digital content and related assets, and granting the requisite rights necessary to ensure continuity of the content and repository services.

#### **Discussion**

A repository's failure threatens the long-term sustainability of a repository's information content. It is not sufficient for the repository to have an informal plan or policy regarding where its data goes should a failure occur. A formal plan with identified procedures needs to be in place.