TRUSTWORTHY REPOSITORIES: AUDIT AND CERTIFICATION (TRAC) CLINE LIBRARY INTERNAL AUDIT, SPRING 2014

Todd Welch & Kelly Phillips

Spring 2014

Table of Contents

Executive Summary

Introduction

Audit and Certification of Trustworthy Digital Repositories (TRAC) is a recommended practice developed by the Consultative Committee for Space Data Systems. The TRAC international standard (ISO 16363:2012) provides institutions with guidelines for performing internal audits to evaluate the trustworthiness of digital repositories, and creates a structure to support external certification of repositories. TRAC establishes criteria, evidence, best practices and controls that digital repositories can use to assess their activities in the areas of organizational infrastructure, digital object management, and technical infrastructure and risk management. The Cline Library at Northern Arizona University has undertaken an internal audit based on TRAC in order to evaluate the policies, procedures and workflows of the existing digital archives and to prepare for the development and implementation of the proposed institutional repository. The following document provides an overview of the results and recommendations produced by this internal audit.

Overview of results and recommendations

The TRAC structure places two pillars at the center of "trustworthiness": *preservation* and *transparency*. While the current digital repository administered by Special Collections and Archives has always faced these concerns, the internal TRAC audit has made it apparent that procedures and documentation both internal and external to the SCA repository need to be reviewed and updated to strengthen these pillars and prepare the best possible foundation for the new institutional repository.

Preservation has always been at the core of traditional archival practice, but the preservation of digital objects requires new approaches and a much higher level of commitment to constant re-evaluation and updating of archival procedures. The audit has highlighted the need for a comprehensive Preservation Strategic Plan that covers both the current and future repositories to ensure that the library can meet its commitments over the long term. The Cline's digital repository team needs to reassess all technical procedures for the handling and potential transformation of digital objects in light of current best practices, and document those workflows and the policies governing them far more thoroughly.

Transparency refers not only to any legal obligations that might exist for a repository, but also to the mutual dependencies and commitments between the repository, its parent institutions, and the designated community of creators, depositors, and users which it serves. Achieving trustworthy transparency will require that the repository team review and amend submission agreements, preservation commitments, and access and use policies. These documents, as well as all documentation of repository procedures affecting the preservation and integrity of digital objects, must be made available to the designated community and any feedback considered.

The full range of new and updated procedures and documentation suggested by this audit create fundamental mechanisms that ensure reliable daily operations in alignment with digital preservation best practices, that enable sufficient oversight to prepare for changes, and that record all decisions and resulting actions for complete transparency. The repository documentation and the practices it describes, however, cannot be static. All policies, procedures and workflows must be evaluated and updated on an ongoing basis to reflect the dynamic environment in which digital archives operate. The repositories must develop effective mechanisms for regularly scheduled reviews and must commit to the expenditure of time and energy required by the process of continual development.

Organizational Infrastructure (TRAC Section 3)

The audit results indicate that work needs to be done from an organizational infrastructure perspective to define both the current digital repository (DR) and the proposed institutional repository (IR). Achieving trustworthy status will require documented commitments, at both the library and the university level, to the set of services that the repositories will provide. These documents must specifically delineate the responsibilities and activities of both repositories.

The library's mission statement should clearly define long-term support of the repositories as central to the library's mission; more specific individual mission statements should also be developed for the DR and IR. Repository staff must review and update the current collection development policy, adding an explicit digital preservation services component. A library-wide Preservation Strategic Plan is a keystone of the TRAC model for trustworthiness, and it is critical that the Cline also develop a comprehensive plan that delineates the repositories' practices while preparing possible responses to future contingencies.

Explicit commitments should be made to hiring and continual development of staff with the necessary skills to provide repository services. The Cline organizational chart should be amended to show staff roles within the structure of the repositories, and staff job descriptions should be developed or amended to reflect repository duties. The library must be able to track repository finances in such a way that administrators can identify and quantify the resources that are devoted to DR/IR activities, including staff time and associated costs.

The audit has revealed that the history of the DR is inadequately documented; the library should act on the opportunity to change practices now, and to establish a complete history of development and decision making for the IR.

The deeds of gift that accompany repository submissions are legal instruments which delineate rights, responsibilities and liabilities. These forms must be reviewed and amended to make sure all preservation rights are specified and transferred, and to explicitly address digital considerations in all aspects of acquisition, maintenance, and withdrawal. The IR, in particular, may face issues of intellectual property and potential restrictions on content use; the repositories must be prepared to manage all deposits per the submission agreements.

As a public institution, the Cline already has a commitment to transparency which must also be seen in repository operations. All policies, procedures, and workflows must be public on the web site, subject to examination and feedback from each repository's designated user community (producers, depositors, researchers, students, and the public). A better environment for transparency, accountability and issue mitigation should be achieved by creating a communication plan and workflow to track and manage each set of submitted data objects. This will also provide the Cline with an opportunity to deepen community relationships by keeping depositors informed throughout the process.

Digital Object Management (TRAC Section 4)

While the DR has developed successfully over the last 17 years, there are procedures, policies, and workflows in the current services that need to evolve to meet changing needs and new best practices. This process of documentation, reassessment and updating will be instrumental in preparing for the launch of the IR service in the coming year.

The repositories need to develop submission agreements that manage the rights to the digital content as above; to achieve full transparency, these agreements must also list the obligations of the producer and library, define processes and procedures that will affect the digital objects, and fully document the object properties to be preserved. These agreements are merely the first step in the documentation chain that must follow the digital object through its lifecycle in the repository, first as the original Submission Information Package (SIP), then in its persistent, preservable form as an Archival Information Package (AIP), and finally as the Dissemination Information Package (DIP) that will be available to users (see figure 1, “Open Archival Information System”, p.6). The documentation must also include the ultimate disposition of any SIPs and AIPS not retained in perpetuity.

Repository staff must create, update, and comprehensively document workflows and procedures that will ensure that the content and contextual information that must be associated with digital objects is preserved and that the integrity and accessibility of the object is maintained; this process will be guided by, and will in turn inform, the overall Preservation Strategic Plan.

The repository must have consistent mechanisms for acquisition and ingest of submitted objects (SIPs) that guarantee the completeness and correctness of the objects. To achieve this, the repository must develop procedures to produce true unique identifiers, to accurately collect the metadata necessary for object access and preservation, and to store that metadata separately from the object; persistent relationships must be created between the metadata and the object in all its forms.

As objects are processed from SIPs into archival digital objects (AIPs), the repository must record all actions and processes relevant to the storage and preservation of the archived object. This record will help make informed decisions possible regarding the transformations necessary to preserve the object over the long term.

Tracking the creation of archived digital objects (AIPs) and enabling their transformation for preservation also requires the development and implementation of an archival format registry. This registry must become part of a larger suite of preservation implementation documents that record and make transparent not only technical details, but also the rationales used and decisions made during the processing of objects within the repositories.

The repository must improve its mechanisms for both quality control and error checking. A regular schedule of checks for metadata and object file integrity must be instituted, and storage conditions, including file redundancy and backup procedures, should be reassessed on a regular basis. The Cline repositories currently use hosted repository and storage platforms; it is incumbent upon the repository staff to continually monitor and evaluate the performance and the suitability of these services.

Policies and procedures for the creation of the object versions that are available to the end-user (DIPs) must also be continually reviewed and updated to guarantee content integrity and usability. Transparency requires that descriptions of these processes must be available to users so that they can understand the exact relationship of the disseminated object to the archived object.

The repositories must also have clear, published access and use policies appropriate to their communities, and to which each repository can document its adherence. The current policy of the DR and the default policy of the IR is to provide full public access in accordance with the Open Access philosophy. The DR's current model of community engagement can also be improved, and the repository team needs to develop more effective mechanisms for eliciting community involvement and feedback, particularly as the library encounters new types of designated communities through the IR services.

Technical infrastructure and risk management (TRAC Section 5)

The technical environment of a digital repository is ever-changing, and a significant component of trustworthiness rests on the ability of the repository to not only provide a suitable technological infrastructure, but also to anticipate potential risks, assess effective responses, and safely implement necessary changes. Staff will need to increase their awareness of emerging technology trends in hardware and software, making technology watch an explicit job function. The library must commit to supporting staff in development activities that will keep the repository abreast of both new technologies and evolving best practices in the digital archives profession.

The library has chosen to use hosted platforms for archival storage (Amazon Web Services) and for archive access (ContentDM for the DR; ePrints for the IR). These providers meet industry standards such

as ISO 9001[1], ISO 17799[2], and ISO 27000[3], which eases the burden on repository staff of performing some infrastructure and risk management functions. The repository management team must, however, make sure that they are fully aware of the repositories' preservation risks and state of recoverability from loss (from corrupted bits to civil disasters), and must be capable of independently analyzing risks and benefits and responding appropriately. Staff must have full documentation and control of the numbers and locations of all digital objects (SIPs, AIPs, and DIPs) in the hosted environments and be able to independently verify the integrity of objects, and must have complete understanding and control of any available backup functionality.

As with all other aspects of repository operation examined in this audit, the technical infrastructure and security of the repositories must be regularly reviewed and changes to policies and procedures made as necessary. The repository team should perform risk/threat/benefit analyses at scheduled intervals and at any critical intermediate point identified via technology watch or other source.

Next steps

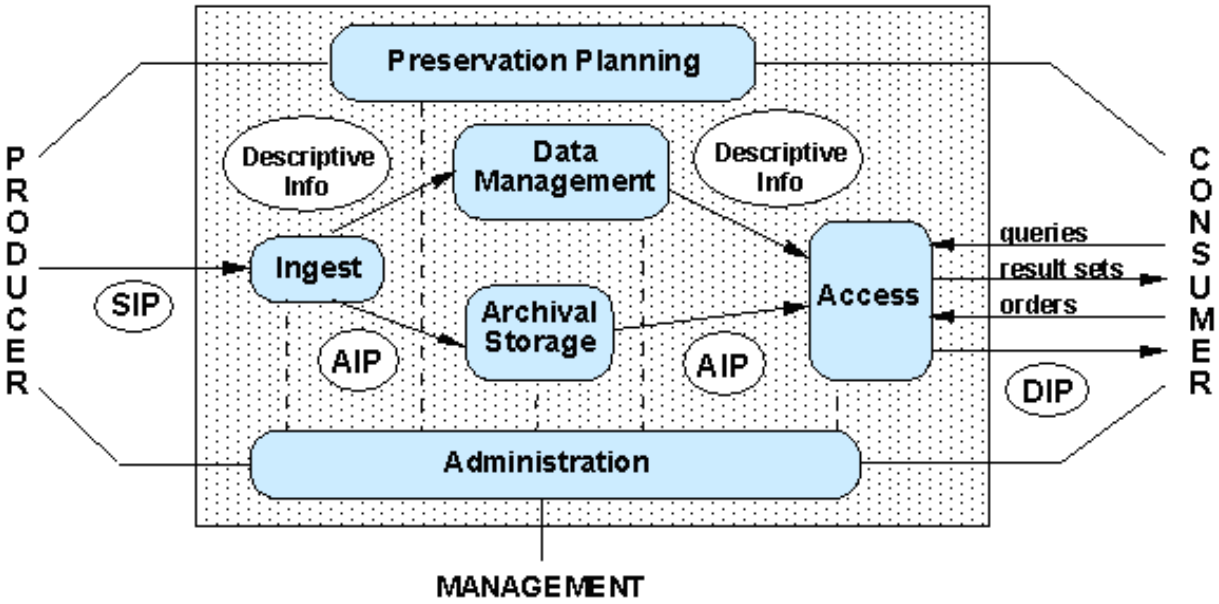
The administration and the repository team should review the detailed results and recommendations of the audit and discuss with internal and external stakeholders. The library should consider purchasing the full ISO 16363:20121 standard document that has evolved from the TRAC initiative. Key players should research and draft documentation defining and articulating the policies and procedures necessary to bring the DR into alignment with the TRAC guidelines and to launch the IR in compliance with best practices for digital archiving and open access.

[1] International Organization for Standardization, ISO 9000 Standards family: Quality management. http://www.iso.org/iso/iso_9000

[2] International Organization for Standardization, ISO/IEC 1799 Standard: Information technology -- Security techniques -- Code of practice for information security management http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=39612

[3] International Organization for Standardization, ISO/IEC 27000 Standards family: Information Security Management http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

Figure 1. Open Archival Information System (OAIS) reference model



Source: Procedures Manual for the Consultative Committee for Space Data Systems (2001)

List of Proposed Documentation

Additional documentation and changes to existing documentation suggested by TRAC audit.

- **Annual or biennial policy review** for both repositories, including review of and update of audit report; assess and alter procedures and policies as needed. 3.3.6

Section 3

- Amendment to library mission statement concerning the commitment to the DR/IR management, preservation, and dissemination of digital content. 3.1.1
- **Preservation Strategic Plan** which coordinates object-level preservation policies and implementation plans with repository- and institutional-level planning for preservation commitment sustainability over the long term. See *Appendix A: Glossary* (pg.32) for suggested preservation plan definitions and structures. 3.1.2
- Amendment to continuity of operation plan that references the activities and functions of the DR/IR in cases of a cessation of operations or budgetary cuts. 3.1.2
- Amendment to the collection policy to specify the types of digital formats and content that the DR will preserve, retain, manage, and provide access to. 3.1.3
- **Collection policy** for the IR. 3.1.3
- **Repository Mission Statements** for both repositories. 3.3.1
- Documentation identifying and defining the skills, staffing, and training necessary to successfully operate each repository. See *Appendix B: SHERPA* document for a representative description of repository staff roles and competencies. 3.2.1
- Identification of staff competencies and duties necessary DR and/or IR operation. 3.2.1.1
- Organizational chart/ delineation of functions specific to repository activities. 3.2.1.2
- Working definitions of the designated community of creators, depositors, and users for the DR and potential designated communities for the IR which are aligned with the repository collection development policies. 3.3.1
- Preservation policy documents applicable to each repository. 3.3.2
- **Preservation Implementation Plan. 3.3.2**
- History/ development document that records early evolution of the IR, with provision to continuously document subsequent development. 3.3.3
- History/development document that recovers as much as possible of the history of the DR, including input from early participants, with provision to continuously document subsequent development. 3.3.3
- Suite of documentation intended for public access expressing the commitments and policies of the DR in language intended for the designated community (this will be developed from other documents in this list). 3.3.4

- Suite of documentation intended for public access expressing the commitments and policies of the DR in language suitable for the designated community (this will be developed from other documents in this list). 3.3.4
- Document describing the schedule for, procedures for, and results of both random and complete integrity verification procedures to be performed on both repositories. Parallel document intended for public access in language suitable for the designated community. 3.3.5
- Subunit (repository-level) budget that accounts for the DR/IR activities within the Library.
- Update the Library's emergency planning documentation to include repository-level concerns, identify possible risks, and establish mitigation processes. 3.4.3
- Amend deposit agreements to include provisions covering digital repository activities, e.g. online access rights, use fees, and preservation/transformation rights for original objects and surrogates; consult with legal counsel on boilerplate for agreements. 3.5.1.1
- Policy and procedure for notifying depositor when formal acceptance of preservation responsibility for digital objects occurs (see Communication Plan). 3.5.1.3
- Policy and process documents for handling liability and challenges to digital objects; e.g. cases of unclear ownership. Consult with legal counsel. 3.5.1.4
- Tracking log for access and use statistics for the IR. 3.5.2

Section 4

- **Content Policies** for both repositories. 4.1
- Amend submission agreements to list the obligations of the Producer and Library, define processing procedures, and delineate the Information Properties of digital information that it will commit to ingesting and preserving. Include language in submission agreement concerning retention, transformation, and disposal of SIPs. 4.1.1, 4.2.3.1
- **Digital Object Transfer form** for collecting information from record producers or depositors about the properties and content of the digital objects in question. 4.1.2
- Procedure and workflow documentation for the examination and confirmation of the SIP characteristics (i.e. file format, formats of any associated metadata, and content verification). 4.1.3
- **Operating Procedures Manual** for both repositories documenting all policies, procedures, workflows for the transformation and ingestion of digital objects, including processes for recording adequate administrative and contextual metadata, tracking transformation activities per digital object, and checking completeness and correctness throughout the intake process. 4.1.4 – 4.1.6
- **Communication Plan** for informing producers/depositors of the ingest process at specific predefined points. 4.1.7

- Administrative action log that that documents the "history" of each digital object ingested into the repositories and records every transformation and action undertaken during ingest and transformation processes (see comprehensive tracking system). 4.1.8
- Definitions for each class of Master File Format and how it will be implemented in each repository. 4.2.1
- Process descriptions for the transformation of SIPs to Master File Formats, including normalization processes to ensure consistent transformation. 4.2.2
- **Comprehensive tracking system** that documents the acceptance, transformation, or disposal of all submitted objects. 4.1.8, 4.2.3, 4.2.10
- Documentation of workflows that describe and verify the accurate application of each repository's unique identifiers. 4.2.4.1
- **File format registry** that documents the Representation Information for the digital objects acquired/ingested at the SIP, AIP, and DIP stages. 4.2.5
- Written procedure for engaging members of designated communities in understandability tests for AIP Content Information. 4.2.7
- Procedure and workflow documentation for verifying the completeness, correctness, and usability of AIPs during creation. 4.2.8
- Specifications for AIP preservation metadata and workflow documentation for metadata extraction and storage. 4.4.1
- Written procedures and schedules for independently verifying AIP file integrity and repository integrity. 4.4.1.2
- **Operating Procedures Manual** for both repositories documenting all policies, procedures, workflows affecting the processing, storage, transformation, integrity checking, and disposal of AIP objects, as well as DIP generation and testing. 4.4.2
- **Access and Use Policies** for both repositories. 4.6.1

Section 5

- **Repository Systems Overview** for each repository, describing the structures, relationships, and dependencies of local systems, hosted storage providers, and hosted access providers, and the protocols, policies, and procedures needed to maintain the repository. Documentation should include file exchange procedures between systems, access mechanisms, and any error checking, data repair, and backup functionality. 5.1
- Document delineating technology watch and hardware/software monitoring and assessment activities. 5.1.1.1
- Procedures for performing risk/benefit and change analyses when considering upgrades or alterations to systems and workflows, or implementation of new systems or workflows. 5.2.2 – 5.2.3

- Amend the library's disaster preparedness and recovery plan to include procedures related to the digital repositories. 5.2.4

Detailed Results and Recommendations

3 Organizational Infrastructure

3.1 Governance & organizational viability

3.1.1 The repository shall have a mission statement that reflects a commitment to the preservation of, long term retention of, management of, and access to digital information.

The repository should draft and propose an addition to the library mission statement concerning the commitment to the DR/IR management, preservation, and dissemination of digital content.

3.1.2 The repository shall have a Preservation Strategic Plan that defines the approach the repository will take in the long-term support of its mission.

The repository must create a Preservation Strategic Plan (see *Appendix A: TRAC Glossary* for a suggested plan definition and structure). The library continuity plan should be amended to explicitly reference the activities and functions of the DR/IR in case of budgetary cuts or a cessation of operations.

3.1.2.1 The repository shall have an appropriate 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.

The library continuity plan should be amended to explicitly reference the activities and functions of the DR/IR in case of budgetary cuts or a cessation of operations.

3.1.2.2 The repository shall monitor its organizational environment to determine when to execute its succession plan, contingency plans, and/or escrow arrangements.

The library administration monitors the organizational environment and determines when it will execute the continuity plan, in response to institutional, university, and state-level financial contingencies.

3.1.3 The repository shall have a Collection Policy or other document that specifies the type of information it will preserve, retain, manage, and provide access to.

The repository needs to amend the collection policy to specify the types of electronic and digital information that the DR will preserve, retain, manage, and provide access to. A collection policy must also be developed for the IR (look at *Appendix B: SHERPA* bullet points for content policy, p.40].

3.2 Organizational Structure and Staffing

3.2.1 The repository shall have identified and established the duties that it needs to perform and shall have appointed staff with adequate skills and experience to fulfill these duties.

The development and implementation of the IR will require library administration to re-evaluate and expand the duties and skills necessary to fulfill its mandate. The identification and definition of the skills, staffing, and training necessary to successfully operate an IR repository will be crucial to future staff planning and organization within the library. See *Appendix B: SHERPA* document.

3.2.1.1 The repository shall have identified and established the duties that it needs to perform.

The repository must identify and document the competencies and duties required for ongoing operation.

3.2.1.2 The repository shall have the appropriate number of staff to support all functions and services.

The repository should develop an organizational chart/delineation of functions specific to DR/IR activities. This structure will also serve to document the expenditure of resources.

3.2.1.3 The repository shall have in place an active professional development program that provides staff with skills and expertise development opportunities.

Recommend establishing an Intranet space for a DR/IR "training" folder that links to continuing training opportunities, professional development, instructions or listserv membership/archive, Internet Resources (e.g. Library of Congress Preservation Directorate and Digital Library Federation).

3.3 Procedural accountability and preservation policy framework

3.3.1 The repository shall have defined its Designated Community and associated knowledge base(s) and shall have these definitions appropriately accessible.

Repository working group should create working definitions of potential designated communities for the DR and IR, starting with the two categories of producers and end-users and working from the specific to the general. These definitions should be aligned with collection development policies for both repositories.

3.3.2 The repository shall have Preservation Policies in place to ensure its Preservation Strategic Plan will be met.

Recommend the current "bits & pieces" of DR/IR policies be surveyed, consolidated, and amended to create Preservation Policy documents applicable to each repository. This documentation should include the development of a Preservation Implementation Plan.

3.3.2.1 The repository shall have mechanisms for review, update, and ongoing development of its Preservation Policies as the repository grows and as technology and community practice evolve.

Recommend surveying the DR/IR policies and consolidate into Preservation Policy documents as per 3.3.2. Set up an annual or biennial policy review to assess and update procedures and policies as needed.

3.3.3 The repository shall have a documented history of the changes to its operations, procedures, software, and hardware.

The library has not deliberately documented the history of the DR. Early participants in the creation of the digital archives should be contacted while possible, to reconstruct initial decision-making and resulting developments. Documents need to be created that record decision-making and actions taken early in the planning and implementation of the IR. For both DR and IR, a commitment should be made and procedures created for tracking subsequent development.

3.3.4 The repository shall commit to transparency and accountability in all actions supporting the operation and management of the repository that affect the preservation of digital content over time. The repository must create a suite of documentation that is intended for public access expressing the commitments and policies of the DR/IR. This will be crucial as the library seeks initial IR 'buy-in' from the faculty.

3.3.5 The repository shall define, collect, track, and appropriately provide its information integrity measurements.

The repository must create schedules for random and complete verification of content integrity (e.g. utilizing the MD5 checksum independent of AWS and CONTENTdm). Specific integrity check procedures and policy workflows should be documented and made publicly accessible.

3.3.6 The repository shall commit to a regular schedule of self-assessment and external certification.

The repository should commit to a regular schedule of self-assessment based on recognized international standards such as ISO 16363, with regular monitoring of the TRAC standard, reviews of literature on digital repository best practices, and research into the certification efforts of comparable repositories. Update or replace the audit spreadsheet and accompanying report on a regular schedule.

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.

Financial and budgetary allocations are at the library and/or departmental (i.e. SCA) level -- not at the sublevel of the digital repository. The Library has not evaluated the budgets of other institutions performing the same functions and activities. Suggest considering the development of a subunit budget that accounts for the DR/IR activities within the Library.

3.4.2 The repository shall have financial practices and procedures which are transparent, compliant with relevant accounting standards and practices, and audited by third parties in accordance with territorial legal requirements.

The implementation of a subunit budget process for the repository will allow for the transparent reporting of financial transactions and activities.

3.4.3 The repository shall have an ongoing commitment to analyze and report on financial risk, benefit, investment, and expenditure (including assets, licenses, and liabilities).

Update the Library's emergency planning documentation to include repository-level concerns, identify possible risks, and establish mitigation processes. Develop process to properly document decisions and actions related to the repository so that accurate analysis and reporting on the investment and expenditure of resources is ensured.

3.5 Contracts, licenses, & liabilities

3.5.1 The repository shall have and maintain appropriate contracts or deposit agreements for digital materials that it manages, preserves, and/or to which it provides access.

SCA should codify (i.e. boilerplate) its agreements to include digital repository activities, online access rights, and use fees. Agreements should be stored in a centralized location for ease of access. When designing a submission agreement with future depositors, sections regarding the management, access, and preservation of the objects must be addressed and explained.

3.5.1.1 The repository shall have contracts or deposit agreements which specify and transfer all necessary preservation rights, and those rights transferred shall be documented.

The agreements must contain access and preservation rights to originals and surrogates. The development of a boilerplate reviewed by legal counsel must be completed in the next year.

3.5.1.2 The repository shall have specified all appropriate aspects of acquisition, maintenance, access, and withdrawal in written agreements with depositors and other relevant parties.

The Deed of Gift covers many aspects of the acquisition, maintenance, and removal of donated materials, but it should be expanded to cover digital objects and rights. A submission agreement should also be attached to Deed of Gifts for digital objects.

3.5.1.3 The repository shall have written policies that indicate when it accepts preservation responsibility for contents of each set of submitted data objects.

Repository must develop a notification to producer/depositor providing confirmation of formal acceptance of contents of the deposited digital objects.

3.5.1.4 The repository shall have policies in place to address liability and challenges to ownership/rights.

The repository must codify a policy and process for handling liability and challenges to digital objects stored and distributed in the system. Policies and procedures for handling digital content with unclear ownership need to be drafted and submitted to university legal counsel for approval.

3.5.2 The repository shall track and manage intellectual property rights and restrictions on use of repository content as required by deposit agreement, contract, or license.

The repository shall develop deposit agreements in coordination with depositors to ensure compliance with legal and university requirements. IR policies should align with the Northern Arizona University Research Data Management Policy: "The goal of data management is to assist Principal Investigators to identify, understand, manage, and apply an appropriate level of security to their research data."

4 Digital Object Management

4.1 Ingest: acquisition of content

4.1.1 The repository shall identify the Content Information and the Information Properties that the repository will preserve.

Both the DR and IR will need to develop submission and transfer agreements that transfer rights to the repository, list the obligations of the Producer and Library, define processing procedures, and document the properties to be preserved. The submission agreement would define aspects of ownership and rights management. A transfer agreement would collection information about the history, context, and content of donated digital objects.

4.1.1.1 The repository shall have a procedure(s) for identifying those Information Properties that it will preserve.

Repository policies must delineate Information Properties of digital information that it will ingest and preserve, as well as clearly describe those Information Properties that it is not committing to preserve (e.g. Content Policy for IR). Significant properties include the characteristics of digital objects that must be preserved over time in order to ensure the continued accessibility, usability, and meaning of the objects, and their capacity to be accepted as evidence of what they purport to record (per Andrew Wilson, National Archives of Australia).

4.1.1.2 The repository shall have a record of the Content Information and the Information Properties that it will preserve.

Repository must keep a record of the application of the Information Property policies for individual submissions.

4.1.2 The repository shall clearly specify the information that needs to be associated with specific Content Information at the time of its deposit.

The repository must create and implement a Digital Object Transfer Form that collects information from record producers or depositors about the properties and content of the digital objects in question. The repository must provide access to this document from its web site. DR/IR should also standardize and record the digital object ingestion workflow per individual object.

4.1.3 The repository shall have adequate specifications enabling recognition and parsing of the SIPs.

Develop written procedures and workflows for the examination and confirmation of the SIP characteristics (e.g. file format and content verification).

4.1.4 The repository shall have mechanisms to appropriately verify the identity of the Producer of all materials.

DR/IR should create a procedure manual for the transformation and ingestion of digital objects, record transforms per digital object, and authenticate/verify checksums throughout the intake process. The workflow for the born-digital objects comprising the John Running Collection is a great case study. The repository must ensure the preservation of administrative and contextual information used to connect/trace the SIP to the producer/ depositor, and record this in the metadata record. Remember and emphasize provenance as a critical part of the workflow.

4.1.5 The repository shall have an ingest process which verifies each SIP for completeness and correctness.

The repository needs to adopt and document a standard ingest workflow for digital objects that generates a registry of files with recorded steps/transformations from donation to ingest. Dedicate a computer workstation to the electronic transfer, transformation, verification, and ingestion of the digital objects to protect the system against viruses. Operating procedures and policies should be written and adopted, as well as regularly reviewed and updated for completeness and robustness. Establish a workstation with appropriate software (BitCurator) to perform digital forensic on submitted materials. Evaluate examples such as the policies, procedures and workflows designed by the DeepBlue Project at the University of Michigan.

4.1.6 The repository shall obtain sufficient control over the Digital Objects to preserve them.

Repository must create a policy and procedure for preserving and maintaining, or properly disposing of, any referenced (external) content "objects." Research how other IRs approach the ingesting and updating of referenced (external) content.

4.1.7 The repository shall provide the producer/depositor with appropriate responses at agreed points during the ingest processes.

Repository needs to establish and implement a communication plan/schedule to inform producers/depositors of the ingest process during specific predefined points.

4.1.8 The repository shall have contemporaneous records of actions and administration processes that are relevant to content acquisition.

Develop a recordkeeping process (i.e. spreadsheet or METS database) that documents the "history" of each digital object ingested into the DR/IR and records every transformation and action undertaken during the ingest process and beyond.

4.2 Ingest: creation of the AIP (Archivable Information Package)

4.2.1 The repository shall have for each AIP or class of AIPs preserved by the repository an associated definition that is adequate for parsing the AIP and fit for long-term preservation needs.

Develop definitions for each class of our Master File Formats and how they are implemented in the DR/IR. Review and update the PDI (Preservation Description Information) extracted from the AIP files and ensure that associated categories are captured: fixity, provenance, context, and reference.

4.2.1.1 The repository shall be able to identify which definition applies to which AIP.

Develop workflow that links AIP metadata field to internal file format registry.

4.2.1.2 The repository shall have a definition of each AIP that is adequate for long-term preservation, enabling the identification and parsing of all the required components within that AIP.

Review and update the PDI extracted from the AIP files and ensure that associated categories are captured: fixity, provenance, context, and reference -- evaluating the adequacy of the data for long-term preservation needs.

With the advent of the IR, research, policies and procedures should be developed for web resources and datasets.

4.2.2 The repository shall have a description of how AIPs are constructed from SIPs.

Create process descriptions and procedures for the transformation of SIPs to our adopted Digital Master File Formats. These descriptions should include normalization processes to ensure consistent transformation.

4.2.3 The repository shall document the final disposition of all SIPs.

Besides continuing the creation and maintenance of the deed of gift/donor files to record actions (i.e. retention, transformation, and disposal) of donated materials, DR/IR should develop a comprehensive tracking system that documents the acceptance, transformation, or disposal of all submitted objects.

4.2.3.1 The repository shall follow documented procedures if a SIP is not incorporated into an AIP or discarded and shall indicate why the SIP was not incorporated or discarded.

Create comprehensive tracking system of ingest and disposition decisions (as above). Include language in submission agreement concerning retention, transformation, and disposal of SIPs.

4.2.4 The repository shall have and use a convention that generates persistent, unique identifiers for all AIPs.

DR/IR should adopt a PURL or ARK system for generating digital master file names.

4.2.4.1 The repository shall uniquely identify each AIP within the repository.
4.2.4.1.1 The repository shall have unique identifiers.
4.2.4.1.2 The repository shall assign and maintain persistent identifiers of the AIP and its components so as to be unique within the context of the repository.
4.2.4.1.3 Documentation shall describe any processes used for changes to such identifiers.
4.2.4.1.4 The repository shall be able to provide a complete list of all such identifiers and do spot checks for duplications.
4.2.4.1.5 The system of identifiers shall be adequate to fit the repository's current and foreseeable future requirements such as numbers of objects.

DR/IR needs to develop documentation and workflows that describe and verify the accurate application of the repository's unique identifiers based on the subcomponents listed above. An analysis of our own DR current practices must be undertaken and recommendations and actions submitted for consideration and implementation.

4.2.4.2 The repository shall have a system of reliable linking/resolution services in order to find the uniquely identified object, regardless of its physical location.

Accurately implement and report the contents of the "location of digital master file" (AIP) field. Develop a workflow for our master digital files (AIPs) that embeds the SIP identifier in the metadata, if the SIP is stored online -- otherwise describe the final disposition. Also add this SIP identifier to the preservation metadata extraction macros that adds the identifier to a METS field (i.e. "SIP identifier").

4.2.5 The repository shall have access to necessary tools and resources to provide authoritative Representation Information for all of the digital objects it contains.

4.2.5.1 The repository shall have tools or methods to identify the file type of all submitted Data Objects.
4.2.5.2 The repository shall have tools or methods to determine what Representation Information is necessary to make each Data Object understandable to the Designated Community.
4.2.5.3 The repository shall have access to the requisite Representation Information.
4.2.5.4 The repository shall have tools or methods to ensure that the requisite Representation Information is persistently associated with the relevant Data Objects.

As part of an established identification and processing workflow, the DR/IR should frequently consult the PRONOM resource to maintain semantic and technical context of the digital objects acquired and ingested into the repositories.

DR/IR should create and maintain a local format registry that documents the Representation Information for the digital objects acquired/ingested at the SIP, AIP, and DIP stages.

4.2.6 The repository shall have documented processes for acquiring Preservation Description Information (PDI) for its associated Content Information and acquire PDI in accordance with the documented processes.

4.2.6.1 The repository shall have documented processes for acquiring PDI.

4.2.6.2 The repository shall execute its documented processes for acquiring PDI.

4.2.6.3 The repository shall ensure that the PDI is persistently associated with the relevant Content Information.

DR/IR must be very mindful of collecting provenance and context information at the time of intake through the Digital Object Transfer Form (whenever possible) and recording the information in the local format registry at the SIP, AIP, and DIP stages. Persistent links to the AIPs are maintained within the METS schema ("location of master digital file" field)

4.2.7 The repository shall ensure that the Content Information of the AIPs is understandable for their Designated Community at the time of creation of the AIP.

4.2.7.1 Repository shall have a documented process for testing understandability for the Designated Communities of the Content Information of the AIPs at their creation.

4.2.7.2 The repository shall execute the testing process for each class of Content Information of the AIPs.

4.2.7.3 The repository shall bring the Content Information of the AIP up to the required level of understandability if it fails the understandability testing.

DR/IR must develop written procedures for engaging and enlisting the expertise of designated/appropriate community members for AIP Content Information understandability testing.

4.2.8 The repository shall verify each AIP for completeness and correctness at the point it is created.

Workflow process should include a checklist of important tasks and settings that must be done to ensure that the handling and transferring of SIPs using md5 checksum verification and that the AIP generation is as complete and correct as possible -- without the process indicating error. Part of the workflow should include opening and displaying the digital object in the designated software.

4.2.9 The repository shall provide an independent mechanism for verifying the integrity of the repository collection/content.

If we generate and implement the documentation, policies, and workflows mentioned in Sections 4.1 and 4.2 correctly, we will not have a need to develop an independent mechanism for ensuring file integrity.

4.2.10 The repository shall have contemporaneous records of actions and administration processes that are relevant to AIP creation.

DR/IR must create and maintain a log of decisions made and actions taken in the creation of AIPs.

4.3 Preservation planning

4.3.1 The repository shall have documented preservation strategies relevant to its holdings.

The repository must create preservation documentation that outlines preservation strategies, workflows, and quality control procedures that conform to the repository's overall preservation strategic plan.

4.3.2 The repository shall have mechanisms in place for monitoring its preservation environment.

The DR will continue passive monitoring of its Designated Community. New procedures for community monitoring must be investigated for the IR, and procedures developed which may depend on the Designated Communities relevant to specific deposits.

4.3.2.1 The repository shall have mechanisms in place for monitoring and notification when Representation Information is inadequate for the Designated Community to understand the data holdings.

The repository should consider adding this activity to an existing staff job description with an accompanying definition of technology watch and evaluation roles and activities. Create prominent feedback opportunities for online users to supply comments and concerns in order to improve understanding of Representation Information among designated communities.

4.3.3 The repository shall have mechanisms to change its preservation plans as a result of its monitoring activities.

After drafting a formal preservation plan and identifying related processes, a regular schedule review of information technologies should be undertaken and the appropriate changes to the preservation plan completed (e.g. not more than five years). Sources to consult should include the LC Preservation Directorate, PRONOM, and the New Zealand National Library. A technology watch plan and process for updating the preservation plan must also be part of the library's long-range preservation planning.

4.3.3.1 The repository shall have mechanisms for creating, identifying or gathering any extra Representation Information required.

Design workflow that compares current Representation Information with best practices as defined by technology watch activities. Sources to consult should include the LC Preservation Directorate, PRONOM, and the New Zealand National Library. A technology watch plan and process for updating the preservation plan must also be part of the library's long-range preservation planning.

4.3.4 The repository shall provide evidence of the effectiveness of its preservation activities.

The repository should continue to generate MD5 checksums and develop a scheduled logging process and procedure for preservation evidence. Planned migration of file formats must be fully investigated and tested before implementation to ensure the understandability of the resultant AIPs, including entering actions in the local file format registry log.

4.4 AIP preservation

4.4.1 The repository shall have specifications for how the AIPs are stored down to the bit level.

Write and maintain documentation describing the preservation metadata extraction and workflow for all AIPs that the repository is committed to preserving.

4.4.1.1 The repository shall preserve the Content Information of AIPs.

Establish repository-level policy and record-keeping practice for preserving and, when necessary, deleting AIPs and DIPS from the system (both access and master files). The DR/IR needs to determine the feasibility and appropriateness of preserving all current and future versions of the AIP.

4.4.1.2 The repository shall actively monitor the integrity of AIPs.

Recommend storing a second copy of each AIP to Glacier and using it for testing fixity or downloading samples throughout the S3 environment, as well as comparing md5 checksums for files stored in CONTENTdm to verify their fixity.

Investigate available tools for generating manifest reports of digital object holdings stored on the Cloud.

Investigate the existence of activity logs on the hosted archive and storage platforms, which would be capable of recording all file actions (i.e. add, modify, duplicate, and delete) to improve tracking.

4.4.2 The repository shall have contemporaneous records of actions and administration processes that are relevant to storage and preservation of the AIPs.

Written documentation of actions and processes related to archival storage must be established and adopted to ensure that preservation activities are implemented consistently throughout the digital repository.

Investigate the existence of an activity log within AWS for recording all file actions (i.e. add, modify, duplicate, and delete) to improve tracking.

4.4.2.1 The repository shall have procedures for all actions taken on AIPs.

Written documentation must be created for any workflow procedures and actions related to AIPs. These procedures should include actions that can be and those that *should not be* performed on an AIP. Training of established and accepted AIP workflows and actions must be performed for new staff and student workers; all staff must be informed and retrained when alterations are made to existing workflows.

4.4.2.2 The repository shall be able to demonstrate that any actions taken on AIPs were compliant with the specification of those actions.

The repository must develop documentation on actions performed against the AIP which is not too cumbersome for staff to accurately and consistently contribute to during ordinary work processes.

4.5 Information management

4.5.1 The repository shall specify minimum information requirements to enable the Designated Community to discover and identify material of interest.

Descriptive metadata practices are performed by staff and provide information that assists in the discoverability of objects: title, date, description, collection name, subjects, places, and pertinent contextual data.

Additional descriptive information, including community specific identifiers, should be gathered at the time of acquisition from the producer or depositor – this will apply particularly to the IR. In the context of the IR, the Designated Community consists of those users with the potential to discover and reuse the academic output of the university community.

4.5.2 The repository shall capture or create minimum descriptive information and ensure that it is associated with the AIP.

The descriptive workflow for the DR and the drafting of descriptions submitted to the IR should be examined for the purpose of effectively and consistently maintaining intellectual control over objects over time. Look at other repositories descriptive metadata standards and use.

4.5.3 The repository shall maintain bi-directional linkage between each AIP and its descriptive information.

The field related to digital object persistent identifier needs to be updated to current digital master file locations. Update documentation reflecting current digitization and ingest workflows.

4.5.3.1 The repository shall maintain the associations between its AIPs and their descriptive information over time.

Metadata exporting from the CONTENTdm software allows administrators to manage and access each master digital object -- once the referential integrity of the files has been restored. Recommend that

metadata and workflows pertaining to referential integrity of IR digital objects are well established and documented before implementation.

4.6 Access management

4.6.1 The repository shall comply with Access Policies.

The DR/IR should establish written access and use policies/statements that should be posted from the online resource pages.

The repository should have an explicit statement defining the limitations on the extent of access and use statistics collected and how they are disseminated. Investigate whether the repository needs to write and adopt a privacy policy for our producers and depositors.

For the IR, establish documentation and services that describe standard access policies, and create a framework for which access policies can be tailored to meet specific access circumstances. Provide appropriate access to ingested resources and generate regular reports on use and downloads of digital objects.

4.6.1.1 The repository shall log and review all access management failures and anomalies.

We should investigate this matter within the CONTENTdm, ePrints, and AWS environments and determine the usefulness of this information from an administrative and operational perspective.

4.6.2 The repository shall follow policies and procedures that enable the dissemination of digital objects that are traceable to the originals, with evidence supporting their authenticity.

The manual processing of DIPs is defined in training and workflow documentation. During the creation of some DIP classes (i.e. photographs and textual objects) alterations are made to the content to enhance the display of the original AIP. The AIP is captured, but not altered. Documentation regarding these workflow procedures should be added to individual objects or posted in general workflow documentation for public consumption. Oral history transcriptions are reviewed and edited per standard departmental procedures. Translations of non-English interviews are generated, but not necessarily authenticated. The working group should discuss the potential challenges presented by IR deposits which have very specific disciplinary content outside of local expertise.

4.6.2.1 The repository shall record and act upon problem reports about errors in data or responses from users.

The IR resources loaded into ePrints will require access testing before and after the initial ingest to ensure that access requests can be satisfied in appropriate ways. Mechanisms for error reporting should be created/evaluated.

5 Infrastructure and Security Risk Management

5.1 Technical infrastructure risk management

5.1.1 The repository shall identify and manage the risks to its preservation operations and goals associated with system infrastructure.

5.1.1.1 The repository shall employ technology watches or other technology monitoring notification systems.

The repository needs to strengthen existing monitoring practices and increase its awareness of hardware and software systems in order to improve alignment with professional best practices.

5.1.1.1.1 The repository shall have hardware technologies appropriate to the services it provides to its designated communities.

Investigate the development of distinct user group profiles that account for different needs, expectations, and uses within each designated community. We accept feedback regarding hardware and service, but there is no systematic solicitation of user feedback. Library maintains a current hardware inventory.

5.1.1.1.2 The repository shall have procedures in place to monitor and receive notifications when hardware technology changes are needed.

Recommend the use of local staff expertise to research and update list of hardware liabilities and recommendations. Annual equipment refreshment schedules and budgets must account for repository workflows and services.

5.1.1.1.3 The repository shall have procedures in place to evaluate when changes are needed to current hardware.

Those components that are managed in-house should be identified and policies and procedures developed and implemented to evaluate current and future hardware needs.

5.1.1.1.4 The repository shall have procedures, commitment and funding to replace hardware when evaluation indicates the need to do so.

The library should develop financial and operational procedures and commitments for replacing hardware based on a regular, systematic review by repository staff.

5.1.1.1.5 The repository shall have software technologies appropriate to the services it provides to its designated communities.

Investigate the development of distinct user group profiles that account for different needs, expectations, and uses within each designated community. We accept feedback regarding software and service, but there is no systematic solicitation of user feedback. Library maintains a current software inventory.

5.1.1.1.6 The repository shall have procedures in place to monitor and receive notifications when software changes are needed.

Software that is managed in-house should be identified and policies and procedures developed and implemented to evaluate current and future software needs. Staff should perform regular evaluation of the interface and functional software of the hosted archive and storage systems.

5.1.1.1.7 The repository shall have procedures in place to evaluate when changes are needed to current software.

Those components that are managed in-house should be identified and policies and procedures developed and implemented to evaluate current and future software needs. Evaluation of hosted systems should include assessment of vendor update success and potential necessity to evaluate other comparable systems.

5.1.1.1.8 The repository shall have procedures, commitment, and funding to replace software when evaluation indicates the need to do so.

The library should develop financial and operational procedures and commitments for replacing software based on a regular, systematic review by repository staff.

5.1.1.2 The repository shall have adequate hardware and software support for backup functionality sufficient for preserving the repository content and tracking repository functions.

Create document defining how AWS (relationship/location of files in S3 and Glacier), CONTENTdm, ePrints, and NAU secure the data and system comprising the DR/IR. The current effort to amend and update the library's disaster preparedness and recovery plan must include procedures related to the digital repositories. Create document describing current METS schema (i.e. checksum values) and system information (i.e. file structure within AWS, CONTENTdm and ePrints). Staff should understand hosted backup functionality.

5.1.1.3 The repository shall have effective mechanisms to detect bit corruption or loss.

Recommend creating written documentation on our existing practices for managing files for reliability and durability. MD5 checksums should be used to independently verify files stored in AWS (via Cloudberry), and to verify the preservation metadata in CONTENTdm; this should occur on a regular schedule. Add to documentation referenced above and mention procedures for detecting, reporting, and repairing corrupt/lost data. AWS performs file "self-healing" when bit corruption/loss has been detected. CONTENTdm does not perform regular verification of file integrity.

5.1.1.3.1 The repository shall record and report to its administration all incidents of data corruption or loss, and steps shall be taken to repair/replace corrupt or lost data.

AWS provides documentation on their processes to detect and repair data corruption/loss, but do not send reports on incidents. CONTENTdm does report incidents of data loss when detected. The DR extracts and saves PDI information in its METS schema for internal/independent tracking and

management purposes, including MD5 checksum values. Also recommend regularly (i.e. quarterly) scheduled exporting CONTENTdm collection metadata into tab-delimited files for redundancy.

5.1.1.4 The repository shall have a process to record and react to the availability of new security updates based on a risk-benefit assessment.

CONTENTdm updates are recorded on the User Support Center website. The hosted server updates are handled by OCLC. AWS and Cloudberry (3rd party) software update documentation and hardware refresh schedules are not readily available. Repository staff must keep track of risks and potential security needs, regularly evaluate vendor systems and procedures, and take any necessary actions.

5.1.1.5 The repository shall have defined processes for storage media and/or hardware change (e.g., refreshing, migration).

DR moved to hosted storage solution (AWS) in spring 2013 to mitigate continual hardware refreshment, maintenance, and replacement. CONTENTdm and OCLC observe the ISO-9001 certified operations practices, including regular evaluation and refreshment of hardware, storage, and networking capabilities. They have redundant architecture in place that allows servers to be brought down/up as needed. Issues are communicated to customers for either planned outages, or in the instance of an unplanned outage.

5.1.1.6 The repository shall have identified and documented critical processes that affect its ability to comply with its mandatory responsibilities.

We must recognize the changes in the broader technology environment, develop the necessary adjustment to the repository needs and requirements, and train staff on the appropriate changes. The working group should establish the mandatory level of service commitments for the repositories and identify the critical processes to meet these responsibilities.

5.1.1.6.1 The repository shall have a documented change management process that identifies changes to critical processes that potentially affect the repository's ability to comply with its mandatory responsibilities.

Recommend developing a traceability matrix to clarify the relationship between repository processes and repository service commitments, as described in the TRAC document.

5.1.1.6.2 The repository shall have a process for testing and evaluating the effect of changes to the repository's critical processes.

All changes to the local software and hardware affecting the SIP AIP and DIP workflows must be thoroughly tested and evaluated prior to incorporation in the repositories' procedures. CONTENTdm has multi-level, off-line testing of updates to its infrastructure environment. Recommend inquiring as to how ePrints handles testing and evaluating changes to a repository's critical processes.

5.1.2 The repository shall manage the number and location of copies of all digital objects.

Recommend creating written documentation on our existing practices for managing files for reliability and durability.

5.1.2.1 The repository shall have mechanisms in place to ensure any/multiple copies of digital objects are synchronized.

Recommend testing the durability of duplicate copies of master files in S3 and Glacier. Find a utility that allows us to do this, but also independently verify with random retrieval of files from Glacier for md5 comparison.

5.2 Security risk management

5.2.1 The repository shall maintain a systematic analysis of security risk factors associated with data, systems, personnel, and physical plant.

Create repository overview document defining how AWS, CONTENTdm, ePrints, and NAU secure the data and system comprising the DR/IR. The documentation should include the protocols, policies, and procedures needed to maintain the repository.

5.2.2 The repository shall have implemented controls to adequately address each of the defined security risks.

Create repository overview document as above; examine systems as documented to create a risk/threat analysis. Plan response for risk factors within in-house systems and practices.

5.2.3 The repository staff shall have delineated roles, responsibilities, and authorizations related to implementing changes within the system.

Create repository systems overview document as above, including a change management analysis. Define staff roles in terms of security access and concerns (see SHERPA document).

5.2.4 The repository shall have suitable written disaster preparedness and recovery plan(s), including at least one off-site backup of all preserved information together with an offsite copy of the recovery plan(s).

Create repository overview document as above, defining backup and restore procedures for AWS (including relationship/location of files in S3 and Glacier), CONTENTdm, ePrints, and NAU systems comprising the DR/IR. The current effort to amend and update the library's disaster preparedness and recovery must include procedures related to the digital repositories.

Appendix A – TRAC Documentation: Introduction and Overview

From the Consultative Committee for Space Data Systems
Recommendation for Space Data System Practices

AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES
RECOMMENDED PRACTICE
CCSDS 652.0-M-1
MAGENTA BOOK

September 2011

AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES
CCSDS 652.0-M-1 Page 1-1 September 2011

1 INTRODUCTION

1.1 PURPOSE AND SCOPE
The main purpose of this document is to define a CCSDS Recommended Practice on which to base an audit and certification process for assessing the trustworthiness of digital repositories. The scope of application of this document is the entire range of digital repositories.

1.2 APPLICABILITY
This document is meant primarily for those responsible for auditing digital repositories and also for those who work in or are responsible for digital repositories seeking objective measurement of the trustworthiness of their repository. Some institutions may also choose to use these metrics during a design or redesign process for their digital repository.

1.3 RATIONALE
In 1996 the Task Force on Archiving of Digital Information (reference [B1]) declared, 'a critical component of digital archiving infrastructure is the existence of a sufficient number of trusted organizations capable of storing, migrating, and providing access to digital collections'. The task force saw that 'trusted' or trustworthy organizations could not simply identify themselves. To the contrary, the task force declared, 'a process of certification for digital archives is needed to create an overall climate of trust about the prospects of preserving digital information'.

Work in articulating responsible digital archiving infrastructure was furthered by the development of the Open Archival Information System (OAIS) Reference Model (reference [1]). Designed to create a consensus on 'what is required for an archive to provide permanent or indefinite long-term preservation of digital information', the OAIS addressed fundamental questions regarding the long-term preservation of digital materials that cut across domain-specific implementations. The reference model (ISO 14721) provides a common conceptual framework describing the environment, functional components, and information objects within a system responsible for the long-term preservation of digital materials. Long before it became an approved standard in 2002, many in the cultural heritage community had adopted OAIS as a model to better understand what would be needed from digital preservation systems.

Institutions began to declare themselves 'OAIS-compliant' to underscore the trustworthiness of their digital repositories. However, there was no established understanding of 'OAIS compliance' beyond being able to apply OAIS terminology to describe their archive, despite there being a compliance section in OAIS which specifies the need to support the model of information and fulfilling the mandatory responsibilities.

Claims of trustworthiness are easy to make but are thus far difficult to justify or objectively prove. Establishing more clear criteria detailing what a trustworthy repository is and is not has become vital.

In 2002, Research Libraries Group (RLG) and Online Computer Library Center (OCLC) jointly published Trusted Digital Repositories: Attributes and Responsibilities (reference [B2]), which further articulated a framework of attributes and responsibilities for trusted, reliable, sustainable digital repositories capable of handling the range of materials held by large and small cultural heritage and research institutions. The framework was broad enough to accommodate different situations, technical architectures, and institutional responsibilities while providing a basis for the expectations of a trusted repository. The document has proven to be useful for institutions grappling with the long-term preservation of cultural heritage resources and has been used in combination with the OAIS as a digital preservation planning tool. As a framework, this document concentrated on high-level organizational and technical attributes and discussed potential models for digital repository certification. It refrained from being prescriptive about the specific nature of rapidly emerging digital repositories and archives and instead reiterated the call for certification of digital repositories, recommending the development of certification program and articulation of auditable criteria.

OAIS included a Roadmap for follow-on standards which included 'standard(s) for accreditation of archives'. It was agreed that RLG and National Archives and Records Administration (NARA) would take this particular topic forward and the later published the TRAC (reference [B3]) document which combined ideas from OAIS (reference [1]) and *Trusted Digital Repositories: Attributes and Responsibilities* (TDR—reference [B2]). The current document follows on from TRAC in order to produce an ISO standard.

1.4 STRUCTURE OF THIS DOCUMENT

This document is divided into informative and normative sections and annexes. Sections 1-2 of this document are informative and give a high-level view of the rationale, the conceptual environment, some of the important design issues, and an introduction to the terminology and concepts.

– Section 1 gives purpose and scope, rationale, a view of the overall document structure, and the acronym list, glossary, and reference list for this document.

– Section 2 provides an overview of audit and certification criteria, ideas about evidence to support claims, and a discussion of related standards.

Metrics are empirically derived and consistent measures of effectiveness. When evaluated together, metrics can be used to judge the overall suitability of a repository to be trusted to provide a preservation environment that is consistent with the goals of the OAIS. Separately, individual metrics or measures can be used to identify possible weaknesses or pending declines in repository functionality.

– Sections 3 to 5 provide the normative metrics against which a digital repository may be judged. These sections provide metrics grouped as follows:

- 3 covers Organizational Infrastructure;
- 4 covers Digital Object Management;
- 5 covers Infrastructure and Security Risk Management.

Each section groups metrics into one or more subsections.

– Security considerations are discussed in annex A.

– Annex B provides Informative References.

1.5 DEFINITIONS

1.5.1 ACRONYMS AND ABBREVIATIONS

AIP	Archival Information Package (defined in reference [1])
CCSDS	Consultative Committee for Space Data Systems
DEDSL	Data Entity Specification Language (see reference [B7])
DIP	Dissemination Information Package (defined in reference [1])
FITS	Flexible Image Transport System
GIS	Geographic Information System
ISO	International Organization for Standardization
OAIS	Open Archival Information System (see reference [1])
PDI	Preservation Description Information (defined in reference [1])
SIP	Submission Information Package (defined in reference [1])
TEI	Text Encoding Initiative
UML	Unified Modeling Language
XML	Extensible Markup Language

1.5.2 TERMINOLOGY

Digital preservation interests a range of different communities, each with a distinct vocabulary and local definitions for key terms. A glossary is included in this document, but it is important to draw attention to the usage of several key terms. In general, key terms in this document have been adopted from the OAIS Reference Model. One of the great strengths of the OAIS Reference Model has been to provide a common terminology made up of terms ‘not already overloaded with meaning so as to reduce conveying unintended meanings’ (reference [1]). Because the OAIS has become a foundational document for digital preservation, the common terms are well understood and are therefore used within this document.

The OAIS Reference Model uses ‘digital archive’ to mean the organization responsible for digital preservation. In this document, the term ‘repository’ or phrase ‘digital repository’ is used to convey the same concept in all instances except when quoting from the OAIS. It is important to understand that in all instances in this document, ‘repository’ and ‘digital repository’ are used to convey digital repositories and archives that have, or contribute to, long-term preservation responsibilities and functionality. This document uses the OAIS concept of the ‘Designated Community’. A repository may have a single, generalized ‘Designated Community’ (e.g., every citizen of a country), while other repositories may have several, distinct Designated Communities with highly specialized needs, each requiring different

functionality or support from the repository; this document uses the term Designated Community to cover this second case also.

Finally, this document names criteria that, combined, evaluate the trustworthiness of digital repositories and archives.

1.5.2.1 Glossary

Unless otherwise indicated, other definitions are taken from the OAIS Reference Model (reference [1]).

Access Policy: Written statement, authorized by the repository management, that describes the approach to be taken by the repository for providing access to objects accessioned into the repository. The Access Policy may distinguish between different types of access rights, for example between system administrators, Designated Communities, and general users.

Practice: Actions conducted to execute procedures. Practices are measured by logs or other evidence that record actions completed.

Preservation Implementation Plan: A written statement, authorized by the management of the repository, that describes the services to be offered by the repository for preserving objects accessioned into the repository in accordance with the Preservation Policy.

NOTE – The relationship between these terms is motivated as follows. A repository is assumed to have an overall Repository Mission Statement, part of which will be concerned with preservation. The Preservation Strategic Plan states how the mission will be achieved, in general terms with goals and objectives. The Preservation Policy then declares the range of approaches that the repository will employ to ensure preservation (that is, to implement the Preservation Strategic Plan), and finally the Preservation Implementation Plan translates those into services that the repository must carry out. This is an abstract documentary model that, in reality, can result in different documents, a different distribution of subjects between documents, different document names, etc.

Preservation Policy: Written statement, authorized by the repository management, that describes the approach to be taken by the repository for the preservation of objects accessioned into the repository. The Preservation Policy is consistent with the Preservation Strategic Plan.

Preservation Strategic Plan: A written statement, authorized by the management of the repository, that states the goals and objectives for achieving that part of the mission of the repository concerned with preservation. Preservation Strategic Plans may include long-term and short-term plans.

Procedure: A written statement that specifies actions required to complete a service or to achieve a specific state or condition. Procedures specify how various aspects of the relevant Preservation Implementation Plans are to be fulfilled.

Provider (or Submitter): A person or system that submits a digital object to the repository. The Provider can be the Producer.

Repository Mission Statement: A written statement, authorized by the management of the repository, that, among other things, describes the commitment of the organization for the stewardship of digital objects in its custody.

1.5.3 NOMENCLATURE

The following conventions apply for the normative specifications in this Recommended Practice:

a) the words 'shall' and 'must' imply a binding and verifiable specification;
b) the word 'should' implies an optional, but desirable, specification;
c) the word 'may' implies an optional specification;
d) the words 'is', 'are', and 'will' imply statements of fact.

NOTE – These conventions do not imply constraints on diction in text that is clearly informative in nature.

1.5.4 CONVENTIONS

The following conventions apply:

– The term Designated Community may include multiple Designated Communities.

– Sub-metrics for any section are intended to help clarify and elucidate their superior item. Satisfaction of the sub-metrics provides evidence supporting a claim of compliance with the hierarchically superior items.

– Each metric has one or more of the following informative pieces of text associated with it:

- Supporting Text: giving an explanation of why the metric is important;
- Examples of Ways the Repository Can Demonstrate It Is Meeting This Requirement: providing examples of the evidence which might be examined to test whether the repository satisfies the metric;
- Discussion: clarifications about the intent of the metric.

1.6 CONFORMANCE

An archive that conforms to this Recommended Practice shall have satisfied the auditor on each of the requirements.

Conformance to these metrics, as with all other such standards, is a matter of judgment. The supporting organization and practice of auditing will lead to the creation of auditors' guidelines, as described in the draft ISO 16919.

As described in the referenced ISO documents, the aim of the audit process is to create a process of continuous improvement. Thus the outcome of the audit will not be a simple yes/no but rather a judgment about areas that need improvement.

1.7 REFERENCES

The following documents contain provisions which, through reference in this text, constitute provisions of this Recommended Practice. At the time of publication, the editions indicated were valid. All

documents are subject to revision, and users of this Recommended Practice are encouraged to investigate the possibility of applying the most recent editions of the documents indicated below. The CCSDS Secretariat maintains a register of currently valid CCSDS documents.

[1] *Reference Model for an Open Archival Information System (OAIS)*. Recommendation for Space Data System Standards, CCSDS 650.0-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, January 2002. [Also published as ISO 14721:2003.]

NOTE – Informative references are listed in annex B.

2 OVERVIEW OF AUDIT AND CERTIFICATION CRITERIA

This section provides an overview of some of the key concepts that are incorporated in the design of the metrics in this Recommended Practice.

2.1 A TRUSTWORTHY DIGITAL REPOSITORY

At the very basic level, the definition of a trustworthy digital repository must start with 'a mission to provide reliable, long-term access to managed digital resources to its Designated Community, now and into the future' (reference [B2]). Expanding the definition has caused great discussion both within and across various groups, from the broad digital preservation community to the data archives or institutional repository communities.

A trustworthy digital repository will understand threats to and risks within its systems. Constant monitoring, planning, and maintenance, as well as conscious actions and strategy implementation will be required of repositories to carry out their mission of digital preservation. All of these present an expensive, complex undertaking that depositors, stakeholders, funders, the Designated Community, and other digital repositories will need to rely on in the greater collaborative digital preservation environment that is required to preserve the vast amounts of digital information generated now and into the future.

Communicating audit results to the public—transparency—will engender more trust, and additional objective audits, potentially leading towards certification, will promote further trust in the repository and the system that supports it. Finally, attaining trustworthy status is not a one-time accomplishment, achieved and forgotten. To retain trustworthy status, a repository will need to undertake a regular cycle of audit and/or certification.

2.2 EVIDENCE

As noted in 1.5.4 each metric has associated with it informative text under the heading *Examples of Ways the Repository Can Demonstrate It Is Meeting This Requirement:* providing examples of the evidence which might be examined to test whether the repository satisfies the metric. These examples are illustrative rather than prescriptive, and the lists of possible evidence are not exhaustive.

2.3 RELEVANT STANDARDS, BEST PRACTICES, AND CONTROLS

Numerous documents and standards include pieces that are applicable or related to this work. These standards are important to acknowledge and embrace as complementary audit tools. A few examples:

– The ISO 9000 family of standards (e.g., *Quality Management Systems— Fundamentals and Vocabulary*—reference [B9]) addresses quality assurance components within an organization and system management that, while valuable, were not specifically developed to gauge the trustworthiness of organizations operating digital repositories.

– Similarly, ISO 17799:2005 (reference [B10]) was developed specifically to address data security and information management systems. Like ISO 9000, it has some very valuable components to it but it was not designed to address the trustworthiness of digital repositories. Its requirements for information security seek data security compliance to a very granular level, but do not address organizational, procedural, and preservation planning components necessary for the long-term management of digital resources.

– ISO 15489-1:2001 and ISO 15489-2:2001 (references [B11] and [B12]) define a systematic and process-driven approach that governs the practice of records managers and any person who creates or uses records during their business activities, treats information contained in records as a valuable resource and business asset, and protects/preserves records as evidence of actions. Conformance to ISO 15489 requires an organization to establish, document, maintain, and promulgate policies, procedures, and practices for records management, but, by design, addresses records management specifically rather than applying to all types of repositories and archives.

– Finally, ISO 14721:2003, the Open Archival Information System Reference Model, provides a high-level reference model or framework identifying the participants in digital preservation, their roles and responsibilities, and the kinds of information to be exchanged during the course of deposit and ingest into and dissemination from a digital repository.

It is important to acknowledge that there is real value in knowing whether an institution is certified to related standards or meets other controls that would be relevant to an audit. Certainly, an institution that has undertaken any kind of certification process—even if none of the evaluated components overlap with a digital repository audit—will be better prepared for digital repository certification. And those that have achieved certification in related standards will be able to use those certifications as evidence during the digital repository audit.

Appendix B – SHERPA Institutional Repositories: Staff and Skills Requirements

SHERPA Document
Institutional Repositories: Staff and Skills requirements

Mary Robinson
University of Nottingham
8th August 2007
Circulation PUBLIC

Introduction

This document began in response to requests received by the core SHERPA team for examples of job descriptions for repository posts. Its development has been greatly assisted by contributions from the SHERPA partners and UKCORR members.

This document will be revised annually (July/August) to reflect changing needs and requirements. Input from the repository community will be sought at this time.

Staff

Staff requirements for a repository vary greatly between institutions depending on the remit of the repository and existing and available resources. In some repositories the skills, knowledge and abilities required may be expected of an individual repository post with the assistance of general IT personnel. However, many institutions spread the work over two main posts:

1. A Repository Manager- who manages the 'human' side of the repository including content policies, advocacy, user training and a liaison with a wide range of institutional departments and external contacts.

2. Repository Administrator- who manages the technical implementation, customisation and management of repository software, manages metadata fields and quality, creates usage reports and tracks the preservation issues.

Other institutions spread the work over several posts or over several departments; typically including library cataloguers, subject librarians, other library, teaching and administrative staff as well as IT services.

Skills

As mentioned above, institutions vary greatly in how the work of the repository is distributed. Hence this document is **not** intended as the skill set required of a particular repository post but rather the skills, knowledge and abilities required for the development and management of a successful institutional repository.

Management

Ability to:

- Manage the repository budget and respond to user needs in line with resources
- Develop a strategy and costing for the future development of the repository
- Source funding opportunities for repository projects where appropriate
- Manage the repository service by identifying goals and future strategies for improvement in the repository service
- Develop workflows to manage the capture, description and preservation etc. of repository outputs
- Manage the day-to-day running of the repository including any mediated-deposit service (if required or possible) or self-archiving by authors
- Coordinate and manage activities of repository personnel and coordinate repository development with associated departments
- Set up test collections and user satisfaction surveys to evaluate the service and report on findings where appropriate
- Monitor deposit; download and other usage indicators to identify the impact and success of the repository and areas for improvement in the service. Produce usage reports where appropriate.
- Manage user expectations to ensure that expected service delivery is achievable
- Handle comments, complaints and relationships if service delivery does not meet user demand. Manage other difficulties as they arise.

Software

Familiarity with:

- Standard web-based software systems including (but not limited to) Unix, Linux, SQL Server, MySQL, SGML, XML, PHP, JAVA, PERL
- At least one major repository software including (but not limited to) EPrints, DSpace, Fedora, OPUS
- Web-based software and databases

Ability to:

- Customise, deploy and manage repository and associated software
- Arrange and carry out testing of the system and evaluate results
- Design and develop repository interface and tools
- Identify and develop value-added services such as community and collection pages in the repository

Metadata

Familiarity with:

- Relevant metadata standards including (but not limited to) Dublin Core, MARC, METS, MODS, OAI-PMH

Ability to:

- Identify or develop appropriate metadata and other standards
- Liaise and test implementation with cataloguing team where appropriate
- Ensure compliance and monitor metadata quality on an ongoing basis

Storage & Preservation

Familiarity with:

- Current best practice procedures and external advice and resources

Ability to:

- Work with IT Services on the use of their network storage and on backup requirements
- Scope the long term storage requirements of repositories and work with IT services to meet backup requirements
- Work with institutional personnel including (but not limited to) University Records Manager, Archivist and IT services, as well as external organisations in order to
    - Identify best practice and establish requirements for preservation
    - Develop a policy for how different materials should be preserved (or not)

Content

Familiarity with:

- Relevant IPR issues
    - Needed when accepting material for the repository
    - Needed to develop guidelines to ensure consistent good practice
    - Must be able to provide advice on relevant IPR issues

Ability to:

- Develop a content policy for the repository to include (but not limited to)
    - The types of materials that can be deposited
    - How different materials should be managed within the repository
    - How embargoed materials are to be managed
    - How withdrawals of deposited items are to be managed
- Increase the amount and quality of items deposited in the repository by
    - Identifying suitable publications for deposit by checking personal and departmental web pages and following the development of new areas of research in the institution
    - Encouraging authors of suitable publications to deposit their work
    - Explaining to authors how to self-archive OR where mediated deposit is provided
    - Asking authors for files from authors and convert to appropriate formats for deposit (e.g. Word to PDF) and deposit in the repository on their behalf

Liaison (Internal)

Ability to:

- Liaise with a wide variety of departments and interest groups (e.g. students) to
    - Identify high-level and longer-term institutional strategies, opportunities and needs of the institution which may be met by the repository
    - Identify and address any areas of concern or overlap between the repository and stakeholder requirements or other interests within the institution
    - Build awareness and confidence in the repository service
    - Develop practical policies and procedures to ensure the repository becomes embedded in the research processes of the institution
- Liaise with a wide variety of departments and interest groups in particular
    - Senior institutional managers must be aware of the benefits of the repository to the institution and must have confidence in the ability of the repository personnel to deliver a key service tailored to the needs of the institution
    - Work with the Research Support/Grants Offices to share information about changing contract and funder requirements
    - Work with IT services to maintain repository hardware and software, to achieve buy-in by IT services into the repository; explain the needs of the repository and to ensure the repository is integrated and aligned with other university systems to deliver services
    - Work with the library to identify key information and services needed by researchers from the repository and to ensure that repository staff are aware of any feedback from users
    - Initiate contact with individual academics and research groups in the institution to identify their needs from the repository and develop their involvement in the repository
    - Where a repository is to hold e-theses, liaise with the Graduate School to encourage/ensure deposit of e-theses and to identify and address any potential copyright issues

Liaison (External)

Ability to:

- Promote the repository outside the institution as a showcase of the institution's work. At a minimum, the repository should be registered with OpenDOAR, OAI and other relevant service providers such as the OAIster and BASE search engines
- Liaise with external stakeholders in open access and repository development, including (but not limited to) funding agencies; publishers; repository groups or federations; service providers; learned societies; international peers and related organisations

Advocacy, Training & Support

Ability to:

- Develop an advocacy programme to address the full spectrum of stakeholders to create a broad culture of engagement within the institution
- Develop advocacy and publicity materials for use within the institution e.g. webpages, guides, FAQs and presentations
- Be proactive in publicizing repository developments via institutional newsletters, seminars and email alerts etc
- Assess the training needs of specific stakeholder groups within the institution
- Develop suitable training programmes and materials for those groups
- Organise and run training sessions. Topics may include (but are not limited to)
    - Introduction to Open Access
    - How to deposit items into the repository
    - How to search for OA materials
- Answer queries and provide advice as appropriate

Current Awareness & Professional Development

Familiarity with:

- Current trends in the repository community, particularly with respect to events within the UK, through attendance at relevant conferences, meeting and reading relevant email lists and professional literature
- Developments within the general research community and the UK higher education system to identify potential implications for the repository
- Technical and repository developments through attendance at relevant workshops and training courses

Ability to:

- Participate (where appropriate) in new developments, best practice, and relevant projects within the repository community

SHERPA Document
Institutional Repositories: Staff and Skills Requirements
Mary Robinson
University of Nottingham
8th August 2007

Appendix C – Cline Internal TRAC Audit – Full Spreadsheet

Audit performed by Todd Welch and Kelly Phillips Spring/Summer 2014. Criteria and evidence drawn from the Consultative Committee for Space Data Systems Recommendation for Space Data System Practices: Audit And Certification Of Trustworthy Digital Repositories Recommended Practice, CCSDS 652.0-M-1 Magenta Book, published September 2011.

Trustworthy Digital Repositories: Audit and Certification

NAU Cline Library Self-Audit

3. Organizational Infrastructure

- 3.1 Governance & organizational viability
- 3.2 Organizational structure & staffing
- 3.3. Procedural accountability & preservation policy fram
- 3.4 Financial sustainability
- 3.5 Contracts, licenses, & liabilities

4. Digital Object Management

- 4.1 Ingest: acquisition of content
- 4.2 Ingest: creation of the AIP
- 4.3 Preservation planning
- 4.4 AIP preservation
- 4.5 Information management
- 4.6 Access management

5. Infrastructure and Security Risk Management

- 5.1 Technical infrastructure risk management
- 5.2 Security risk management

3.1 Governance & organizational viability			Notes
	3.1.1 The repository shall have a mission statement that reflects a commitment to the preservation of, long term retention of, management of, and access to digital information.		
	Evidence: Mission statement or charter of the repository or its parent organization that specifically addresses or implicitly calls for the preservation of information and/or other resources under its purview; a legal, statutory, or government regulatory mandate applicable to the repository that specifically addresses or implicitly requires the preservation, retention, management and access to information and/or other resources under its purview.		
Evidence Examined:	**Findings and observations:**	**Result/recommendation:**	
Mission statement for library. Context of digital repository within library setting. (Nancy Pitz/Laura Taylor)	Mission statement (Laura). See if DR/IR is connected with NAU/Cline mission statement. The Library contributes to the body of knowledge related to the Colorado Plateau by offering traditional and Web-based reference services, acquiring and making available new collections, adding to the Colorado Plateau Archives, assisting with curriculum development, interpreting resources through exhibitions and presentations, and by reaching out to users to introduce the excitement of conducting research with original materials. Special Collections also houses the University Archives -- a collection which captures the story of over 100 years of higher education in northern Arizona -- and the archival collections of the Arizona Historical Society/Northern Division, the Hopi Cultural Preservation Office, and the Grand Canyon Historical Society.	The repository should draft and propose an addition to the library mission statement concerning the commitment to the DR/IR management, preservation, and dissemination of digital content.	
	3.1.2 The repository shall have a Preservation Strategic Plan that defines the approach the repository will take in the long-term support of its mission.		
	Evidence: Preservation Strategic Plan; meeting minutes; documentation of administrative decisions which have been made.		
Evidence Examined:	**Findings and observations:**	**Result/recommendation:**	
	Under development. No succession plan. 2014-15 specific continuity of operation plan.	The repository must create a Preservation Strategic Plan. The library continuity plan should be amended to explicitly reference the activities and functions of the DR/IR in case of budgetary cuts or a cessation of operations.	

	3.1.2.1 The repository shall have an appropriate 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.													
		Evidence: 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.												
			Under development. No succession plan. 2014-15 specific continuity of operation plan.					The library continuity plan should be amended to explicitly reference the activities and functions of the DR/IR in case of budgetary cuts or a cessation of operations.						
	3.1.2.2 The repository shall monitor its organizational environment to determine when to execute its succession plan, contingency plans, and/or escrow arrangements.													
		Evidence: Administrative policies, procedures, protocols, requirements; budgets and financial analysis documents; fiscal calendars; business plan(s); any evidence of active monitoring and preparedness.												
per conversation with Nancy Pitz & Peter Runge								The library administration monitors the organizational environment and determines when it will execute the continuity plan, in response to institutional, university, and state-level financial contingencies.						

	3.1.3 The repository shall have a Collection Policy or other document that specifies the type of information it will preserve, retain, manage, and provide access to.													
		Collection policy and supporting documents; Preservation Policy, mission goals and vision of the repository.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
SCA collection policy				Current collection policy defines subject areas and formats that SCA does and does not collect. [DOAR collection policy documents]					The repository needs to amend the collection policy to specify the types of electronic and digital information that the DR will preserve, retain, manage, and provide access to. A collection policy must also be developed for the IR.					

3.2 Organizational Structure and Staffing			Notes
	3.2.1 The repository shall have identified and established the duties that it needs to perform and shall have appointed staff with adequate skills and experience to fulfill these duties.		
	No separate evidence. See 3.2.1.1 and 3.2.1.2 below.		
	3.2.1.1 The repository shall have identified and established the duties that it needs to perform.		
	Evidence: A staffing plan; competency definitions; job description; staff professional development plans; certificates of training and accreditation; plus evidence that the repository review and maintains these documents as requirements evolve.		
Todd Welch (student/staff roles(SOR/SOE/Goals)); job descriptions and training budget (Admin.);	No formal plan on training structure or budget. No competency definitions.	The repository must identify and document the competencies and duties required for ongoing operation.	
	3.2.1.2 The repository shall have the appropriate number of staff to support all functions and services.		
	Evidence: Organizational charts; definitions of roles and responsibilities; comparison of staffing levels to industry benchmarks and standards.		
Evidence Examined:	**Findings and observations:**	**Result/recommendation:**	
Organizational chart (SharePoint); need digital repository staffing chart; people/time dependencies per functions	Organizational chart does not provide definitions or roles specific to DR. No comparison of staffing levels with requirements. People/time dependencies regarding DR activities not defined.	The repository should develop an organizational chart/delineation of functions specific to DR/IR activities. This structure will also serve to document the expenditure of resources.	

	3.2.1.3 The repository shall have in place an active professional development program that provides staff with skills and expertise development opportunities.													
		Evidence: Professional development plans and reports; training requirements and training budgets, documentation of training expenditures (amount per staff); performance goals and documentation of staff assignments and achievements, copies of certificates awarded.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
MWDL, Amigos, DAS, SAA - bulletins.				No formal plan on training structure or budget. External opportunities do exist, but staff and management must be proactive to keep informed of training opportunities.					Recommend establishing a Intranet space for DR/IR "training" folder that links to continuing training opportunities, professional development, instructions or listserv membership/archive, Internet Resources (i.e. Library of Congress Preservation Directorate and Digital Library Federation).					

3.3 Procedural accountability and preservation policy framework														Notes
	3.3.1 The repository shall have defined its Designated Community and associated knowledge base(s) and shall have these definitions appropriately accessible.													
		Evidence: A written definition of the Designated Community.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
MOU (HCPO and AHS, G.C.H.S.); Grand Canyon Association; NAU??				Designated groups include NAU community, Plateau special interests groups, educators, scholars, donors, and professional archivists. Look at online SCA collection development policies. (Check library mission statement for identified stakeholders).					Repository working group should create working definitions of potential designated communities for the DR and IR, starting with the two categories of producers and end-users and working from the specific to the general. These definitions should be aligned with collection development policies for both repositories.					
	3.3.2 The repository shall have Preservation Policies in place to ensure its Preservation Strategic Plan will be met.													
		Evidence: Preservation Policies; Repository Mission Statement.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
Piecemeal - SharePoint; discuss with Peter Runge				"Bits & pieces" of DR's policies are scattered and should be consolidated, updated, and/or documented. Some uploading, indexing, and display components are handled by external vendor.					Recommend the "Bits & Pieces" of DR/IR policies be surveyed and consolidated into Preservation Policy documents applicable to each repository. This documentation should include the development of a Preservation Implementation Plan.					

	3.3.2.1 The repository shall have mechanisms for review, update, and ongoing development of its Preservation Policies as the repository grows and as technology and community practice evolve.													
		Evidence: Current and past written documentation in the form of Preservation Policies, Preservation Strategic Plans and Preservation Implementation Plans, procedures, protocols, and workflows; specifications of review cycles for documentation; documentation detailing reviews, surveys and feedback. If documentation is embedded in system logic, functionality should demonstrate the implementation of policies and procedures.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
Piecemeal - SharePoint; discuss with Peter Runge				DR's current policies are scattered and should be consolidated, updated, and/or documented. Some uploading, indexing, and display components are handled by external vendor.					Recommend surveying the DR/IR policies and consolidate into Preservation Policy documents as per 3.3.2. Set up an annual or biennial policy review to assess and update procedures and policies as needed.					
	3.3.3 The repository shall have a documented history of the changes to its operations, procedures, software, and hardware.													
		Evidence: Capital equipment inventories; documentation of the acquisition, implementation, update, and retirement of critical repository software and hardware; file retention and disposal schedules and policies, copies of earlier versions of policies and procedures; minutes of meetings.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
per Todd Welch				No process has been created for documenting the history of changes during the 17-year existence of the DR. The repository does extract and store preservation metadata for objects in the DR, but has not had to plan or implement a migration or refreshment of data.					The library has not deliberately recorded or documented the history and development of the digital archives. The establishment of the IR is an opportunity to begin anew with a high-profile repository. Repository should also talk with early participants of digital archives to record earlier stages of its history. Recommend creating document that records early decisions of IR (with provision to continuously document evolve of the IR). Work on documenting history of digital archives and commit to tracking subsequent development.					

	3.3.4 The repository shall commit to transparency and accountability in all actions supporting the operation and management of the repository that affect the preservation of digital content over time.													
		Evidence: Comprehensive documentation that is readily accessible to stakeholders; unhindered access to content and associated information within repository.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
				Repository is committed to future transparency and the establishment of a communication plan that improves accountability in the future operation and management of the DR/IR.					The repository must create a suite of documentation that is intended for public access expressing the commitments and policies of the DR/IR. This will be crucial as the library seeks initial IR 'buy-in' from the faculty.					
	3.3.5 The repository shall define, collect, track, and appropriately provide its information integrity measurements.													
		Evidence: Written definition or specification of the repository's integrity measures (for example, computed checksum or hash value); documentation of the procedures and mechanisms for monitoring integrity measurements and for responding to results of integrity measurements that indicate digital content is at risk; an audit process for collecting, tracking, and presenting integrity measurements; Preservation Policy and workflow documentation.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
per Todd Welch				Repository has the ability to perform manifest and integrity checks on digital master files; however, there is no established schedule for random, periodic, or complete verification of the content on AWS' Simple Storage Solution. Initial uploads to AWS are "compared"/verified during process. No written policies have been established.					The repository must create schedules for random and complete verification of content integrity (i.e. utilizing the MD5 checksum independent of AWS and CONTENTdm). Add specific integrity check procedures and policy workflows should be documented and made publicly accessible. ["Borrow" AWS language related to data durability and availability.]					

	3.3.6 The repository shall commit to a regular schedule of self-assessment and external certification.													
		Evidence: Completed, dated checklists from self-assessments and/or third-party audits; certificates awarded for compliance with relevant ISO standards; timetables and evidence of adequate budget allocations for future certification.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
				The repository is not currently seeking external certification.					The repository should commit to a regular schedule of self-assessment based on recognized international standards such as ISO 16363, with regular monitoring of the TRAC standard, reviews of literature on digital repository best practices, and research into the certification efforts of comparable repositories. Update or replace this spreadsheet and accompanying report on a regular schedule.					

3.4 Financial sustainability														Notes
	3.4.1 The repository shall have short- and long-term business planning processes in place to sustain the repository over time.													
		Evidence: 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..												
Evidence Examined:				**Findings and observations:**				**Result/recommendation:**						
Nancy Pitz/Peter Runge - do we have a dedicated budget for the Digital Archives -hardware, software, storage, and staffing				The library does have short and long term financial plans, which are dependent on continued support from the state of Arizona. The library performs regular reporting to institutional and state entities and there are regularly scheduled state-mandated audit processes. Local account reports and forecasts are available on request. Neither the library or the repository does directed comparisons with peer institutions. No documented exposure of business plan to scenarios had taken place.				Financial and budgetary allocations are at the library and/or departmental (i.e. SCA) level -- not at the sublevel of the digital repository. The Library has not evaluated the budgets of other institutions performing the same functions and activities. Suggest considering the development of a subunit budget that accounts for the DR/IR activities within the Library.					
	3.4.2 The repository shall have financial practices and procedures which are transparent, compliant with relevant accounting standards and practices, and audited by third parties in accordance with territorial legal requirements.													
		Evidence: Demonstrated dissemination requirements for business planning and practices; citations to and/or examples of accounting and audit requirements, standards, and practice; audited annual financial statements.												
Evidence Examined:				**Findings and observations:**				**Result/recommendation:**						
Nancy Pitz via Peter Runge				The repository and the library, as state institutions, are required to conduct business transparently under the oversight of the state comptroller. All financial activities are subject to public inquiry.				The implementation of a subunit budget process for the repository will allow for the transparent reporting of financial transactions and activities.					

	3.4.3 The repository shall have an ongoing commitment to analyze and report on financial risk, benefit, investment, and expenditure (including assets, licenses, and liabilities).													
		Evidence: Risk management documents that identify perceived and potential threats and planned or implemented responses (a risk register); technology infrastructure investment planning documents; cost/benefit analyses; financial investment documents and portfolios; requirements for and examples of licenses, contracts, and asset management; evidence of revision based on risk.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
per conversation with Nancy Pitz and Peter Runge				The library does have an emergency planning procedure and performs some risk assessment. Values and risks for SCA, including both the physical and digital collections, are particularly hard to assess, and may not be covered by current planning or insurance instruments (e.g. there is no provision in current planning for staff costs to reassemble the DR and reinstate online operations). Some provisions affecting risk may exist in current contracts, licenses, and service agreements.					Update the Library's emergency planning documentation to include repository-level concerns that identifies possible risks and establishes mitigation processes. Develop process to properly document decisions and actions related to the repository so that accurate analysis and reporting on the investment and expenditure of resources is ensured.					

3.5 Contracts, licenses, & liabilities	Notes
3.5.1 The repository shall have and maintain appropriate contracts or deposit agreements for digital materials that it manages, preserves, and/or to which it provides access.	
Evidence: Properly signed and executed deposit agreements and licenses in accordance with local, national, and international laws and regulations; policies on third-party deposit arrangements; definitions of service levels and permitted uses; repository policies on the treatment of 'orphan works' and copyright dispute resolution; reports of independent risk assessments of these policies; procedures for regularly reviewing and maintaining agreements, contracts, and licenses.	

Evidence Examined:	**Findings and observations:**	**Result/recommendation:**	
HCPO/AHS - MOU; Navajo Nation Museum	A current contract exists with the AHS. An agreement with the Hopi lapsed one year ago, but operations continue according to its provisions. Previous agreements existed with the Navajo, but are now an open question. Use fee contracts are maintained in some cases (Kolb, Muench, Grand Canyon River Guides, AHS, HCPO). Other obligations may exist per individual deed of gift. Other situations to check: Grand Canyon River Guides, Michael Collier/GCHA, Grand Canyon Association?	SCA should codify (i.e. boilerplate) its agreements to include digital repository activities, online access rights, and use fees. Agreements should be stored in a centralized location for ease of access. When designing a submission agreement with future donors, sections regarding the management, access, and preservation of the objects must be addressed and explained.	

3.5.1.1 The repository shall have contracts or deposit agreements which specify and transfer all necessary preservation rights, and those rights transferred shall be documented.	
Evidence: Contracts, deposit agreements; specification(s) of rights transferred for different types of digital content (if applicable); policy statement on requisite preservation rights.	

Evidence Examined:	**Findings and observations:**	**Result/recommendation:**	
Look at MOUs, Deeds of Gift, Look at Lew Steiger agreement for rights/restrictions	(Implicit?) Provisions included in the deed of gift in most cases. For AHS, however, digitized material is beyond the current terms of contract. Digitization and preservation rights are also unspecified in Hopi agreements	The agreements must contain access and preservation rights to originals and surrogates. The development of a boilerplate reviewed by legal counsel must be completed in the next year.	

	3.5.1.2 The repository shall have specified all appropriate aspects of acquisition, maintenance, access, and withdrawal in written agreements with depositors and other relevant parties.													
		Evidence: Submission agreements/deposit agreements/deeds of gift; written standard operating procedures.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
Look at MOUs, Deeds of Gift				Aspects of acquisition, maintenance, access, and withdrawal are specified in the repository's deposit/ submission agreements. More explicit terms would be desirable regarding digital objects and rights. Standard operating procedures for the DR and the IR should be developed and/or properly documented.					The Deed of Gift covers many aspects of the acquisition, maintenance, and removal of donated materials, but it should be expanded to cover digital objects and rights. A submission agreement should also be attached to Deed of Gifts for digital objects.					
	3.5.1.3 The repository shall have written policies that indicate when it accepts preservation responsibility for contents of each set of submitted data objects.													
		Evidence: Properly executed submission agreements, deposit agreements, and deeds of gift; confirmation receipt sent back to producer/depositor.												
Deed of Gift states that legal rights have been transferred to repository for digitization and electronic access through the World Wide Web.				Upon transformation and ingestion, the repository accepts preservation responsibility of the donated digital objects. This is not explicitly stated in the deed of gift, but is demonstrated through the workflow process.					Repository must develop a formal notification to producer/depositor providing confirmation of formally acceptance of contents of the deposited digital objects.					

3.5.1.4 The repository shall have policies in place to address liability and challenges to ownership/rights.			
Evidence: A definition of rights, licenses, and permissions to be obtained from producers and contributors of digital content; citations to relevant laws and regulations; policy on responding to challenges; documented track record for responding to challenges in ways that do not inhibit preservation; records of relevant legal advice sought and received.			
Evidence Examined:	**Findings and observations:**	**Result/recommendation:**	
Repository tracks challenges and determine risk/liability before determining whether to continue online access or remove challenged items.	The DR currently handles challenges on a case-by-case basis. A clear and consistent procedure for documenting challenges and resulting actions and outcomes needs to be developed. Policies (and some decisions?) may need to be clarified/cleared through the Dean - Provost - Legal Counsel chain.	The repository must codify a policy and process for handling liability and challenges to digital objects stored and distributed in the system. Policies and procedures for handling digital content with unclear ownership needs to be adopted.	
3.5.2 The repository shall track and manage intellectual property rights and restrictions on use of repository content as required by deposit agreement, contract, or license.			
Evidence: A Preservation Policy statement that defines and specifies the repository's requirements and process for managing intellectual property rights; depositor agreements; samples of agreements and other documents that specify and address intellectual property rights; documentation of monitoring by repository over time of changes in status and ownership of intellectual property in digital content held by the repository; results from monitoring, metadata that captures rights information.			
Evidence Examined:	**Findings and observations:**	**Result/recommendation:**	
Permission to Use, discuss with Peter Runge/Jess Vogelsang	Current deed of gift/ submission agreement terms adequately cover intellectual property concerns for the DR. Procedures, policies and roles need to be further developed for the potentially more complicated situation regarding rights and challenges for content in the IR.	The current repository tracks reproduction and use of digital objects on a quarterly basis and reports to various stakeholders. With the IR, it will be crucial that the Library manage and distribute use of deposited content to faculty and colleges.	

4.1 Ingest: acquisition of content				Notes
	4.1.1 The repository shall identify the Content Information and the Information Properties that the repository will preserve.			
	Evidence: Mission statement; submission agreements/deposit agreements/deeds of gift; workflow and policy documents, including written definition of properties as agreed in the deposit agreement/deed of gift; written processing procedures; documentation of properties to be preserved.			
Evidence Examined:	**Findings and observations:**	**Result/recommendation:**		
Some of this documentation exists in SharePoint, but none of it is complete and it has not updated in the last 5 years.	This has been an issue with recent collections such as John Running, Gary Emmanuel, and Bruce Hooper.	DR/IR will need to develop submission/transfer agreements that transfers rights to the DR/IR, lists the obligations of the Producer and Library, defines processing procedures, and documents the properties to be preserved.		
	4.1.1.1 The repository shall have a procedure(s) for identifying those Information Properties that it will preserve.			
	Evidence: Definitions of the Information Properties which should be preserved; submission agreements/deposit agreements, Preservation Policies, written processing procedures, workflow documentation.			
Evidence Examined:	**Findings and observations:**	**Result/recommendation:**		
per Todd Welch		Repository must delineate Information Properties of digital information that it will ingest and preserve, as well as clearly describe those Information Properties that it is not committing to preserve. (i.e. Content Policy for IR).		
	4.1.1.2 The repository shall have a record of the Content Information and the Information Properties that it will preserve.			
	Evidence: Preservation Policies, processing manuals, collection inventories or surveys, logs of Content Information types, acquired preservation strategies, and action plans.			
Evidence Examined:	**Findings and observations:**	**Result/recommendation:**		
		Repository must keep a record of the application of the Information Property Policies for individual submissions.		

	4.1.2 The repository shall clearly specify the information that needs to be associated with specific Content Information at the time of its deposit.														
		Evidence: Transfer requirements; producer-archive agreements; workflow plans to produce the AIP.													
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**						
				This is very important information to collect at the time of deposit for ingest in the digital repositories. This has been an issue when attempting to process born-digital donations.					The repository must create and implement a "Digital Object" Transfer Form that collects information from record producers or depositors about the properties and content of the digital objects in question. The repository must provide access to this document from its web site. DR/IR should also standardize and record the digital object ingestion workflow per individual object.						
	4.1.3 The repository shall have adequate specifications enabling recognition and parsing of the SIPs.														
		Packaging Information for the SIPs; Representation Information for the SIP Content Data, including documented file format specifications; published data standards; documentation of valid object construction.													
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**						
									Develop written procedures and workflows for the examination and confirmation of the SIP characteristics (i.e. file format and content verification).						
	4.1.4 The repository shall have mechanisms to appropriately verify the identity of the Producer of all materials.														
		Evidence: Legally binding submission agreements/deposit agreements/deeds of gift, evidence of appropriate technological measures; logs from procedures and authentications.													
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**						
Deed of Gift				Deed of Gift should have attachment (submission agreement) containing information on the provenance of deposited materials - this has not been the case often. The staff should also record any workflow or data transformation that altered the properties of donated materials.					DR/IR should create a procedures manual for the transformation and ingestion of digital objects, record transforms per digital object, and authenticate/verify checksums throughout the intake process. The workflow for the born-digital objects comprising the John Running Collection is a great case study.					[correlation not exact] Ensure the preservation of administrative and contextual information that connects/traces the SIP to the Producer/ depositor. Provenance.	

	4.1.5 The repository shall have an ingest process which verifies each SIP for completeness and correctness.													
		Evidence: Appropriate Preservation Policy and Preservation Implementation Plan documents and system log files from system performing ingest procedure; formal or informal "acquisitions register" of files received during the transfer and ingest process; workflow, documentation of standard operating procedures, detailed procedures; definition of completeness and correctness, probably incorporated in policy documents.											
Evidence Examined:			**Findings and observations:**					**Result/recommendation:**						
per Todd Welch			The METS metadata schema records the md5 checksum for each digital object ingested into the digital repository.					The repository needs to document and adopt a standard ingest workflow for digital objects that generates a "registry" of files with recorded steps/transformations from donation to ingest. Dedicate a computer workstation to the electronic transfer, transformation, verification, and ingestion of the digital objects to protect the system against viruses. Operating procedures and policies should be written and adopted, as well as regularly reviewed and updated for completeness and robustness.					[Digital forensic machine] [explore Magenta discussion]
	4.1.6 The repository shall obtain sufficient control over the Digital Objects to preserve them.													
		Evidence: Submission agreements/deposit agreements/deeds of gift; workflow documents; system log files from the system performing ingest procedures; logs of files captured during Web harvesting.												
Evidence Examined:			**Findings and observations:**					**Result/recommendation:**						
Current deed of gift			Deed of gift transfers physical and intellectual control over donated objects, unless restrictions or other conditions have been set by the donor and agreed to by the repository.					Repository must create a policy and procedure for preserving and maintaining (or NOT) the referenced (external) content "objects." Research how other IRs approach the ingesting and updating referenced (external) content.						

4.1.7 The repository shall provide the producer/depositor with appropriate responses at agreed points during the ingest processes.

Evidence: Submission agreements/deposit agreements/deeds of gift; workflow documentation; standard operating procedures; evidence of 'reporting back' such as reports, correspondence, memos, or emails.

Evidence Examined:	Findings and observations:	Result/recommendation:
per Todd Welch	Currently, the repository contacts donors regarding privacy or third-party confidentiality issues that arise with donated materials. There is not a communication plan in place that establishes a schedule of reports to be sent to the producer/depositor of the digital objects.	Repository needs to establish and implement a communication plan/schedule to inform producers/depositors of the ingest process during specific predefined points.

4.1.8 The repository shall have contemporaneous records of actions and administration processes that are relevant to content acquisition.

Evidence: Written documentation of decisions and/or action taken; preservation metadata logged, stored, and linked to pertinent digital objects, confirmation receipts sent back to providers.

Evidence Examined:	Findings and observations:	Result/recommendation:
per Todd Welch	Repository does not currently formally record the transformation process of digital objects in the preservation metadata schema.	Develop a recordkeeping process (i.e. spreadsheet or METS database) that documents the "history" of each digital objects ingested into the DR/IR that records every transformation and actions undertaken during the ingest process and beyond.

4.2 Ingest: creation of the AIP (Archivable Information Package)

4.2.1 The repository shall have for each AIP or class of AIPs preserved by the repository an associated definition that is adequate for parsing the AIP and fit for long-term preservation needs.

Evidence: No separate evidence for 4.2.1

Evidence Examined:	Findings and observations:	Result/recommendation:
Repository has a variety of documentation (mostly dated) that refers to benchmarks, PDI metadata extraction, and digital capture. There are also some dated documents related to born-digital donations and a technical worksheet.		Develop definitions for each class of our Master File Formats and how they are implemented in the DR/IR. Review and update the PDI extracted from the AIP files and ensure that associated categories are captured: fixity, provenance, context, and reference.

4.2.1.1 The repository shall be able to identify which definition applies to which AIP.

Evidence: Documentation clearly linking each AIP, or class of AIPs, to its definition.

		Develop and document workflow that links AIP metadata field to internal file format registry.

4.2.1.2 The repository shall have a definition of each AIP that is adequate for long-term preservation, enabling the identification and parsing of all the required components within that AIP.

Evidence: Demonstration of the use of the definitions to extract Content Information and PDI (Provenance, Access Rights, Context, Reference, and Fixity Information) from AIPs. It should be noted that the Provenance of a digital object, for example, may be extended over time to reflect additional preservation actions.

Evidence Examined:	Findings and observations:	Result/recommendation:
See 4.2.1 for documentation, but there are benchmarks and workflows defined for the following classes: images, textual materials, sound, moving images, large-format objects.	DR/IR needs to work through and document a best practice for converting born-digital objects, as well as discuss archiving web resources and datasets.	Review and update the PDI extracted from the AIP files and ensure that associated categories are captured: fixity, provenance, context, and reference -- evaluating the adequacy of the data for long-term preservation needs. With the advent of the IR - research, policies and procedures should be developed for web resources and datasets.

4.2.2 The repository shall have a description of how AIPs are constructed from SIPs.

Evidence: Process description documents; documentation of the SIP-AIP relationship; clear documentation of how AIPs are derived from SIPs.

Evidence Examined:	Findings and observations:	Result/recommendation:
per Todd Welch	Repository has experience and identified workflows for converting SIPs into the adopted AIP formats, but documentation outlining established, consistent procedures and workflows is lacking.	Create process descriptions and procedures for the transformation of SIPs to our adopted Digital Master File Formats. These descriptions should include normalization processes to ensure consistent transformation.

4.2.3 The repository shall document the final disposition of all SIPs.

Evidence: No separate evidence for 4.2.3

Evidence Examined:	Findings and observations:	Result/recommendation:
Repository has a well-established deed of gift process.	Born-digital collections are reviewed and appraised by curatorial staff soon after accessioning. Staff include LTS personnel in decision-making process. Objects are transformed into AIPs or disposal is recorded in the donor file. See Gary Emanuel and John Running collections.	Besides continuing the creation and maintenance of the deed of gift/donor files to record actions (i.e. retention, transformation, and disposal) of donated materials, DR/IR should develop a comprehensive tracking system that documents the acceptance, transformation, or disposal of all submitted objects.

4.2.3.1 The repository shall follow documented procedures if a SIP is not incorporated into an AIP or discarded and shall indicate why the SIP was not incorporated or discarded.

Evidence: System processing files; disposal records; donor or depositor agreements/deeds of gift; provenance tracking system; system log files; process description documents; documentation of SIP relationship to AIP; clear documentation of how AIPs are derived from SIPs; documentation of standard/process against which normalization occurs; documentation of normalization outcome and how the resulting AIP is different from the SIP(s).

		Create comprehensive tracking system of ingest and disposition decisions (as above). Include language in submission agreement concerning retention, transformation, and disposal of SIPs.

	4.2.4 The repository shall have and use a convention that generates persistent, unique identifiers for all AIPs.													
		Evidence: Documentation describing naming convention and physical evidence of its application (e.g., logs).												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
per Todd Welch				The repository has a naming convention for all types of objects. The system is part of staff and student training. Unfortunately, the file naming convention does not generate unique identifiers (i.e. simple numerical files without institutional code). Department assigns unique call number identifiers to analog materials.					DR/IR should adopt a PURL or ARK system for generating digital master file names.					
	4.2.4.1 The repository shall uniquely identify each AIP within the repository.													
		Evidence: Documentation describing naming convention and physical evidence of its application (e.g., logs).												
per Todd Welch				While the DR has procedures which meet its current needs for object identifiers, it does not have procedures for creating unique identifiers which entirely fulfill this requirement.					DR/IR need to develop documentation and workflows that describe and verify the accurate application of repository's unique identifiers.					4.2.4.1.1 The repository shall have unique identifiers. 4.2.4.1.2 The repository shall assign and maintain persistent identifiers of the AIP and its components so as to be unique within the context of the repository. 4.2.4.1.3 Documentation shall describe any processes used for changes to such identifiers. 4.2.4.1.4 The repository shall be able to provide a complete list of all such identifiers and do spot checks for duplications.

4.2.4.2 The repository shall have a system of reliable linking/resolution services in order to find the uniquely identified object, regardless of its physical location.			
Evidence: Documentation describing naming convention and physical evidence of its application (e.g., logs).			
Evidence Examined:	**Findings and observations:**	**Result/recommendation:**	
per Todd Welch	Repository does not have a formal system for tracking/associating the SIP with the resultant AIP.	Accurately implement and report the contents of the "location of digital master file" (AIPs) field. Develop workflows for our master digital files (AIPs) that embeds the SIP identifier in the metadata, if the SIP is stored online -- otherwise describe the final disposition. Also add this SIP identifier to the preservation metadata extraction macros that adds the identifier to a METS field (i.e. "SIP identifier").	
4.2.5 The repository shall have access to necessary tools and resources to provide authoritative Representation Information for all of the digital objects it contains.			
Evidence: Subscription or access to registries of Representation Information (including format registries); viewable records in local registries (with persistent links to digital objects); database records that include Representation Information and a persistent link to relevant digital objects.			
Evidence Examined:	**Findings and observations:**	**Result/recommendation:**	
per Todd Welch	Metadata is extracted during digital process through a series of dialog boxes and a macro. Representation Information is stored in CONTENTdm and can be used to manage digital objects stored in AWS. During the processing and ingest of the Gary Emanuel Collection, repository staff consulted the PRONOM resource provided by the UK National Archives. There is no established policy or procedure for using a set of tools to establish an authoritative semantic of the digital objects. The repository staff also consult the digitalpreservation.gov site (LC Sustainability of Digital Formats).	As part of an established identification and processing workflow, the DR/IR should frequently consult the PRONOM resource to maintain semantic and technical context of the digital objects acquired and ingested into the repositories. DR/IR should create and maintain a local format registry that documents the Representation Information for the digital objects acquired/ingested at the SIP, AIP, and DIP stages.	4.2.5.1 The repository shall have tools or methods to identify the file type of all submitted Data Objects. 4.2.5.2 The repository shall have tools or methods to determine what Representation Information is necessary to make each Data Object understandable to the Designated Community. 4.2.5.3 The repository shall have access to the requisite Representation Information. 4.2.5.4 The repository shall have tools or methods to ensure that the requisite Representation Information is persistently associated with the relevant Data Objects.

	4.2.6 The repository shall have documented processes for acquiring Preservation Description Information (PDI) for its associated Content Information and acquire PDI in accordance with the documented processes.													
		Evidence: Standard operating procedures; manuals describing ingest procedures; viewable documentation on how the repository acquires and manages Preservation Description Information (PDI); creation of checksums or digests, consulting with Designated Community about Context.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
per Todd Welch				Metadata is extracted during digital process through a series of dialog boxes and a macro. Representation Information is stored in CONTENTdm and can be used to manage digital objects stored in AWS. Donor files contain as much context and provenance information that can be ascertained at the time of intake.					DR/IR must be very mindful of collecting provenance and context information at the time of intake through the Digital Object Transfer Form (whenever possible) and records the information in the local format registry at the SIP, AIP, and DIP stages. Persistent links to the AIPs are maintained within the METS field ("location of master digital file" field)					4.2.6.1 The repository shall have documented processes for acquiring PDI. 4.2.6.2 The repository shall execute its documented processes for acquiring PDI. 4.2.6.3 The repository shall ensure that the PDI is persistently associated with the relevant Content Information.
	4.2.7 The repository shall ensure that the Content Information of the AIPs is understandable for their Designated Community at the time of creation of the AIP.													
		Evidence: Test procedures to be run against the digital holdings to ensure their understandability to the defined Designated Community; records of such tests being performed and evaluated; evidence of gathering or identifying Representation Information to fill any intelligibility gaps which have been found; retention of individuals with the discipline expertise.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
per Todd Welch				In the past, the repository has reached out to outside community member to assist in retaining/supplementing/interpreting information content; however, this has not been a standard or regular basis -- only on a case-by-case basis.					DR/IR must develop written documentation on the workflows and processes necessary to engage and enlist the expertise of designated/appropriate community members.					4.2.7.1 Repository shall have a documented process for testing understandability for their Designated Communities of the Content Information of the AIPs at their creation. 4.2.7.2 The repository shall execute the testing process for each class of Content Information of the AIPs. 4.2.7.3 The repository shall bring the Content Information of the AIP up to the required level of understandability if it fails the understandability testing.

	4.2.8 The repository shall verify each AIP for completeness and correctness at the point it is created.													
		Evidence: Description of the procedure that verifies completeness and correctness; logs of the procedure.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
per Todd Welch				No systematic procedures are in place to verify the completeness and correctness at the time of creation, but errors messages alerting staff of issues associated with AIP creation would begin a review and troubleshooting process with LTS. The repository staff do generate a md5 checksum to verify the file integrity.					Workflow process should include a checklist of important tasks and settings that must be done to ensure that the handling and transferring of SIPs using checksum verification and that the AIP generation is as complete and correct as possible -- without the process indicating error. Part of the workflow should include opening and displaying the digital object in the designated software.					
	4.2.9 The repository shall provide an independent mechanism for verifying the integrity of the repository collection/content.													
		Evidence: Documentation provided for 4.2.1 through 4.2.4; documented agreements negotiated between the producer and the repository (see 4.1.1-4.1.8); logs of material received and associated action (receipt, action, etc.) dates; logs of periodic checks.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
per Todd Welch				The repository does create a log of materials received, but does not record associated or subsequent actions according to any standard procedure or established policy. Repository does negotiate deed of gifts with producers of digital objects as a standard operating procedure. Review Gary Emanuel and John Running deeds.					If we generate and implement the documentation, policies, and workflows mentioned in Sections 4.1 and 4.2 correctly, we will not have a need to develop an independent mechanism for ensuring file integrity.					

	4.2.10 The repository shall have contemporaneous records of actions and administration processes that are relevant to AIP creation.													
		Evidence: Written documentation of decisions and/or action taken with timestamps; preservation metadata logged, stored, and linked to pertinent digital objects.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
per Todd Welch				Library does not consistently track decisions related to actions taken. Preservation metadata is extracted and stored for preservation of AIPs.					DR/IR must create and maintain a log of decisions made and actions taken in the creation of AIPs.					

4.3 Preservation planning														Notes
	4.3.1 The repository shall have documented preservation strategies relevant to its holdings.													
		Evidence: Documentation identifying each preservation issue and the strategy for dealing with that issue.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
Per Todd Welch				No established written documentation. We have standard master file formats per class (i.e. photo, text, sound, moving image). We also used standard redundancy storage settings for digital master files on Amazon's Simple Server Solution, as well as generate a MD5 checksum that can independent of AWS S3 verify the digital integrity and authenticity.					The repository must create preservation documentation that outlines preservation strategies, workflows, and quality control procedures.					
	4.3.2 The repository shall have mechanisms in place for monitoring its preservation environment.													
		Evidence: Surveys of the Designated Community of the repository.												
per Todd Welch				The DR currently engages community members in specific projects, and responds on a case-by-case basis to feedback from the Designated Community, but does not actively survey the community to anticipate changes in technology or use.					The DR will continue passive monitoring of its Designated Community. New procedures for community monitoring must be investigated for the IR, and procedures developed which may depend on the Designated Communities relevant to specific deposits.					

4.3.2.1 The repository shall have mechanisms in place for monitoring and notification when Representation Information is inadequate for the Designated Community to understand the data holdings.

Evidence: Subscription to a Representation Information registry service; subscription to a technology watch service, surveys amongst its Designated Community members, relevant working processes to deal with this information.

Evidence Examined:	Findings and observations:	Result/recommendation:
per Todd Welch	No percentage of a staff role has been specifically identified or allocated to monitor, record, and report on potential or impending technology obsolescence.	The repository should consider adding this activity to an existing staff job description with an accompanying definition of technology watch and evaluation roles and activities. Create prominent feedback opportunities for online users to supply comments and concerns in order to improve understanding of representation Information among designated communities.

4.3.3 The repository shall have mechanisms to change its preservation plans as a result of its monitoring activities.

Evidence: Preservation Plans tied to formal or informal technology watch(es); preservation planning or processes that are timed to shorter intervals (e.g., not more than five years); proof of frequent Preservation Policies and Preservation Plans updates; sections of Preservation Policies that address how plans may be updated and that address how often the plans are required to be reviewed and reaffirmed or updated.

Evidence Examined:	Findings and observations:	Result/recommendation:
per Todd Welch	There is no formal mechanism established to monitor information technology developments and edit the non-exist preservation plans. If an individual is identified to perform this role, their responsibilities would include reporting on recommended responses to the preservation team.	After drafting a formal preservation plan and identify related processes - a regular schedule review of information technologies should be undertaken and the appropriate changes to the preservation plan completed (e.g. not more than five years). Sources to consult should include the LC Preservation Directorate, PRONOM, and the New Zealand National Library. A technology watch plan and process for updating the preservation plan must also be part of the library's long-range preservation planning.

	4.3.3.1 The repository shall have mechanisms for creating, identifying or gathering any extra Representation Information required.													
		Subscription to a format registry service; subscription to a technology watch service; preservation plans.												
									Design workflow that compares current Representation Information with environment best practices as defined by technology watch services. Sources to consult should include the LC Preservation Directorate, PRONOM, and the New Zealand National Library. A technology watch plan and process for updating the preservation plan must also be part of the library's long-range preservation planning.					
	4.3.4 The repository shall provide evidence of the effectiveness of its preservation activities.													
		Evidence: Collection of appropriate preservation metadata; proof of usability of randomly selected digital objects held within the system; demonstrable track record for retaining usable digital objects over time; Designated Community polls.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
Per Todd Welch				MD5 checksums were generated for all digital objects residing in the repository in 2004. The curators can independently verify the accuracy and integrity of the digital objects over the last decade. These objects have migrated from two to three storage media and are still accessible, viewable, and useable with standard portal technology and software.					The repository should continue to generate MD5 checksums and develop a scheduled logging process and procedure for preservation evidence. Planned migration of file formats must be fully investigated and tested before implementation to ensure the understandability of the resultant AIPs, including entering actions in the local file format registry log.					

4.4 AIP preservation														Notes
	4.1 Repository employs documented preservation strategies.													
		Evidence: Documentation of strategies and their appropriateness to repository objects; evidence of application (e.g., in preservation metadata); see B3.3.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
per Todd Welch				The repository extracts preservation metadata that is stored separately from the digital object to allow for integrity checking and authentication. There are no documented repository policies and practices that reflect preservation strategies; however, the repository can employ strategies based on metadata extraction/collection workflows that are performed during object ingestion.					The repository should establish a written preservation plan with workflows identifying the essential tasks and activities involved in digital object(s) preservation.					
	4.2 Repository implements/responds to strategies for archival object (i.e., AIP) storage and migration.													
		Evidence: Institutional technology and standards watch; demonstration of objects on which a preservation strategy has been performed; demonstration of appropriate preservation metadata for digital objects.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
per Todd Welch				There are no established repository-level policies or practices that define strategies or responses to object-based preservation and transformation techniques or activities. The repository has not consistently recorded transformation/migration of object file formats in the past.					Repository-level policies and practices should be developed and implemented to ensure that object-based preservation techniques and migration activities are recorded. A log of specific transformations and migrations should be kept for each object.					

	4.4.1 The repository shall have specifications for how the AIPs are stored down to the bit level.													
		Evidence: Documentation of the format of AIPs; EAST and Data Entity Dictionary Specification Language (DEDSL) descriptions of the data components (see references [B6] and [B7]).												
per Todd Welch				The DR does not currently have this type of fully documented specification.					Document as part of Preservation Implementation Plan per Section 3.2.2.					
	4.4.1.1 The repository shall preserve the Content Information of AIPs.													
		Evidence: Preservation workflow procedure documentation; workflow procedure documentation; Preservation Policy documents specifying treatment of AIPs and under what circumstances they may ever be deleted; ability to demonstrate the sequence of conversions for an AIP for any particular digital object or group of objects ingested; documentation linking ingested objects and the current AIPs.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
per Todd Welch				In the past, objects stored in the repository (access and master copies) have been deleted based on copyright, privacy, cultural sensitivity and collecting scope concerns. The repository has followed collection development and deed of gift guidelines. There is no established chain of custody or log for actions taken once an object has been ingested.					Establish repository-level policy and record-keeping practice for preserving and, when necessary, deleting AIPs from the system (both access and master files). The DR/IR needs to determine the feasibility and appropriateness of preserving all current and future versions of the AIP.					

	4.4.1.2 The repository shall actively monitor the integrity of AIPs.													
		Evidence: Fixity information (e.g., checksums) for each ingested digital object/AIP; logs of fixity checks; documentation of how AIPs and Fixity information are kept separate; documentation of how AIPs and accession registers are kept separate.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
per Todd Welch				Digital objects stored locally are compared with uploaded S3 objects after initial ingest using the CloudBerry utility. The repository has not developed a workflow that regularly samples AIPs. Fixity information (i.e. MD5 checksums) are stored separately in the METS schema and can be independently verified outside of the AWS/Cloudberry environment. Ask Mike about generated manifest reports and the verification of a directory's content stored in S3.					Recommend either storing a second copy in Glacier and using it for testing fixity or downloading samples throughout the S3 environment, as well as comparing md5 checksums stored in CONTENTdm to verify their fixity. Investigate available tools for generating manifest reports of digital object holdings stored on the Cloud. Investigate the existence of an "activity log" recording all file actions (i.e. add, modify, duplicate, and delete) to improve tracking.			
	4.4.2 The repository shall have contemporaneous records of actions and administration processes that are relevant to storage and preservation of the AIPs.													
		Evidence: Written documentation of decisions and/or action taken; preservation metadata logged, stored, and linked to pertinent digital objects.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
per Todd Welch				The repository's METS metadata schema using PREMIS fields to log preservation metadata and maintain a link to the master digital objects. These fields need to be updated to current digital master file locations.					Written documentation of actions and processes related to archival storage must be established and adopted to ensure that preservation activities are implemented consistently throughout the digital repository. Investigate the existence of an "activity log" within AWS for recording all file actions (i.e. add, modify, duplicate, and delete) to improve tracking.			

4.4.2.1 The repository shall have procedures for all actions taken on AIPs.

Written documentation describing all actions that can be performed against an AIP.

Evidence Examined:	Findings and observations:	Result/recommendation:
		Written documentation must be created for any workflow procedures and actions related to AIPs. These procedures should include actions that can and those that *should not be* performed against an AIP. Training of established and accepted AIP workflows and actions must be performed for new staff and student workers.

4.4.2.2 The repository shall be able to demonstrate that any actions taken on AIPs were compliant with the specification of those actions.

Preservation metadata logged, stored, and linked to pertinent digital objects and documentation of that action; procedural audits of the repository showing that all actions conform to the documented processes.

		The repository must develop documentation on actions performed against the AIP which are not too cumbersome for staff to accurately and consistently contribute.

4.5 Information management														Notes
	4.5.1 The repository shall specify minimum information requirements to enable the Designated Community to discover and identify material of interest.													
		Evidence: Retrieval and descriptive information, discovery metadata, such as Dublin Core, and other documentation describing the object.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
Repository's METS schema employed Dublin Core descriptive fields that librarians and staff enter and the Digital Access Librarian samples for quality assurance. Controlled vocabulary fields are maintained and their review occurs annually.				Recently added a non-indexed historical note that contains contextual information. This removed descriptions that lead to misleading "false" hits that lead to frustration among our designated communities.					Descriptive metadata practices are performed by staff and provide information that assists in the discoverability of objects: title, date, description, collection name, subjects, places, and pertinent contextual data. Additional descriptive information could be gathered at the time of acquisition by adding content information specifically to collect community specific identifiers.					
	4.5.2 The repository shall capture or create minimum descriptive information and ensure that it is associated with the AIP.													
		Evidence: Descriptive metadata; internal or external persistent, unique identifier or locator that is associated with the AIP (see also 4.2.4 about persistent, unique identifier); system documentation and technical architecture; depositor agreements; metadata policy documentation, incorporating details of metadata requirements and a statement describing where responsibility for its procurement falls; process workflow documentation.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
per Todd Welch				The repository collects and keeps thorough donor files and correspondence descriptive information on donated objects. The repository also produces collection inventories (EAD guides) that provide hierarchical descriptions and preserves associated/related information on aggregate objects. The METS schema uses identifier fields for call number and collection name that maintains permanent association. Workflows are established and staff/students are trained to capture/create this information.					The descriptive workflow for the DR and the drafting of the completion of descriptions submitted to the IR should be examined with an eye to effectively and consistently maintaining intellectual control over objects over time. Look at other repositories descriptive metadata standards and use.					

4.5.3 The repository shall maintain bi-directional linkage between each AIP and its descriptive information.

Evidence: Descriptive metadata; unique, persistent identifier or locator associated with the AIP; documented relationship between the AIP and its metadata; system documentation and technical architecture; process workflow documentation.

Evidence Examined:	Findings and observations:	Result/recommendation:
per Todd Welch	The METS schema has the ability to maintain the referential integrity between the master digital objects and the associated descriptive information, but the move to AWS has broken the persistent links and should be updated.	The field related to digital object persistent identifier needs to be updated to current digital master file locations. Update documentation reflecting current digitization and ingest workflows.

4.5.3.1 The repository shall maintain the associations between its AIPs and their descriptive information over time.

Evidence: Log detailing ongoing maintenance or checking of the integrity of the data and its relationships to the associated descriptive information, especially following repair or modification of the AIP; legacy descriptive information; persistence of identifier or locator; documented relationship between AIP and its descriptive information; system documentation and technical architecture; process workflow documentation.

Evidence Examined:	Findings and observations:	Result/recommendation:
Metadata exporting from the CONTENTdm software allows administrators to manage and access each master digital object -- once the referential integrity of the files has been restored.	The field related to digital object persistent identifier needs to be updated to current digital master file locations.	Metadata exporting from the CONTENTdm software allows administrators to manage and access each master digital object -- once the referential integrity of the files has been restored. Recommend that metadata and workflows pertaining to referential integrity of IR digital objects are well established and documented before implementation.

4.6 Access management			Notes
	4.6.1 The repository shall comply with Access Policies.		
	Evidence: Statements of policies that are available to the user communities; information about user capabilities (authentication matrices); logs and audit trails of access requests; explicit tests of some types of access.		
Evidence Examined:	**Findings and observations:**	**Result/recommendation:**	
All materials uploaded to the repository are free and open to all users. No separate agreements applicable to access conditions are necessary.	Access policies for the DR/IR should be drafted and adopted that outline the intent and use of the ingested materials in the respective repository.	The DR/IR should establish written access and use policies/statements that should be posted from the online resource pages. The repository should have an explicit statement defining the limitations on the extent of access and use statistics collected and how they are disseminated. Privacy policy for our users? For the IR, establish documentation and services that describes standard access policies, and creates a framework for which access policies can be tailored to meet specific access circumstances. Provide appropriate access to ingested resources and generate regular reports on use and downloads of digital objects.	
	4.6.1.1 The repository shall log and review all access management failures and anomalies.		
	Evidence: Access logs, capability of the system to use automated analysis/monitoring tools and generate problem/error messages; notes of reviews undertaken or action taken as a result of reviews.		
Evidence Examined:	**Findings and observations:**	**Result/recommendation:**	
We do not have access to an audit log of access requests through CONTENTdm.	We should explore how Google Analytics captures access requests to determine if we do indeed have reliable logs of access requests. What about AWS? -- if access failures occur, does Google Analytics and AWS track them? If yes, we should monitor failure occurrences and determine if we can "fix" the access issues that occur.	We should investigate this matter within the CONTENTdm, Eprints, and AWS environments and determine the usefulness of this information from an administrative and operational perspectives.	

	4.6.2 The repository shall follow policies and procedures that enable the dissemination of digital objects that are traceable to the originals, with evidence supporting their authenticity.													
		Evidence: System design documents; work instructions (if DIPs involve manual processing); process walkthroughs; production of a sample copy with evidence of authenticity; documentation of community requirements for evidence of authenticity.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
Generation of the access files is handled by staff and student workers and quality control using digital benchmarks and playback software is undertaken before uploading to CONTENTdm. The manual processing of DIPs is defined in training and workflow documentation.				The steps outline the creation of the access files from the digital master files (AIPs). Some of the preservation metadata captures the location and checksums of the master digital files (i.e. location of digital master file and MD5 checksum) -- and can be independently verified. Oral history transcriptions are reviewed and edited per standard departmental procedures. Translations of non-English interviews are generated, but not necessarily authenticated.					The manual processing of DIPs is defined in training and workflow documentation. During the creation of some DIP classes (i.e. photographs and textual objects) alterations are made to the content to enhance the display of the original AIP. The AIP is captured, but not altered. Documentation regarding this workflow procedure should be added to individual objects or posted in general workflow documentation for public consumption. Make sure that DIP generation workflows and QC are in written documentation. Workflow documentation should be revisited and updated based on technology and user expectations. Are there IR implications that we should consider?				

	4.6.2.1 The repository shall record and act upon problem reports about errors in data or responses from users.													
		Evidence: System design documents; work instructions (if DIPs involve manual processing); process walkthroughs; logs of orders and DIP production; documentation of error reports and the actions taken.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
per Todd welch				DIPs are uploaded after testing into CONTENTdm. The delivery of the DIP is controlled by the hosted site. We have determined that there is an issue with mp4 video files and are working with the vendor to correct. If issues occur with access to particular files, they are discovered by staff during the descriptive metadata activity. We also receive and act on user-generated feedback regarding performance issues with DIPs already in our system.					The IR resources loaded into EPrints will also require access testing before and after the initial ingest to ensure that access requested are satisfied.					

5.1 Technical infrastructure risk management														Notes
	5.1.1 The repository shall identify and manage the risks to its preservation operations and goals associated with system infrastructure.													
		Evidence: Infrastructure inventory of system components; periodic technology assessments; estimates of system component lifetime; export of authentic records to an independent system; use of strongly community supported software e.g., Apache, iRODS, Fedora); re-creation of archives from backups.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
				No consistent, comprehensive documentation of systems or procedures. The library has chosen to pursue "hosted solutions" for storage/backup/data integrity management, off-loading some infrastructure considerations. Further comments in this section refer to in-house operations unless specified.					A repository systems overview document should be created for each repository, describing the structures, relationships, and dependencies of local systems, hosted storage providers, and hosted access providers, and the protocols, policies, and procedures needed to maintain the repository.					
	5.1.1.1 The repository shall employ technology watches or other technology monitoring notification systems.													
		Evidence: Management of periodic technology assessment reports. Comparison of existing technology to each new assessment.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
				No organized system of technology watch.					The repository needs to strengthen existing monitoring practices and increase its awareness of hardware and software systems in order to improve alignment of professional best practices.					[explore tech watch processes at other institutions and businesses]

5.1.1.1.1 The repository shall have hardware technologies appropriate to the services it provides to its designated communities.

Evidence: Maintenance of up-to-date Designated Community technology, expectations, and use profiles; provision of bandwidth adequate to support ingest and use demands; systematic elicitation of feedback regarding hardware and service adequacy; maintenance of a current hardware inventory.

Evidence Examined:	Findings and observations:	Result/recommendation:
Current operations of DR per Todd Welch	The DR accepts feedback regarding service, but there is no systematic solicitation of user feedback. Library maintains a current hardware inventory.	Investigate the development of distinct user group profiles that account for different needs, expectations, and use within each designated community.

5.1.1.1.2 The repository shall have procedures in place to monitor and receive notifications when hardware technology changes are needed.

Evidence: Audits of capacity versus actual usage; audits of observed error rates; audits of performance bottlenecks that limit ability to meet user community access requirements; documentation of technology watch assessments; documentation of technology updates from vendors.

Evidence Examined:	Findings and observations:	Result/recommendation:
	No repository-level hardware audit procedures. Ad-hoc monitoring based on observed performance and user feedback.	Recommend the use of local staff expertise to research and update list of hardware liabilities and recommendations. Annual equipment refreshment schedules and budgets must account for repository workflows and services.

5.1.1.1.3 The repository shall have procedures in place to evaluate when changes are needed to current hardware.

Evidence: Evaluation procedures in place; documented staff expertise in each technology subsystem.

Evidence Examined:	Findings and observations:	Result/recommendation:
	NAU ITS has hardware evaluation and refresh procedures, but there is no formal repository-level evaluation.	Those components that are managed in-house should be identified and polices and procedures developed and implemented to evaluate current and future hardware needs.

5.1.1.1.4 The repository shall have procedures, commitment and funding to replace hardware when evaluation indicates the need to do so.

Evidence: Statement of commitment to provide expected and contracted levels of service; evidence of ongoing financial assets set aside for hardware procurement; demonstration of cost savings through amortized cost of new system.

Evidence Examined:	Findings and observations:	Result/recommendation:
		The library should develop financial and operational procedures and commitments for replacing hardware based on a regular, systematic review by repository staff.

5.1.1.1.5 The repository shall have software technologies appropriate to the services it provides to its designated communities.

Evidence: Maintenance of up-to-date Designated Community technology, expectations, and use profiles; provision of software systems adequate to support ingest and use demands; systematic elicitation of feedback regarding software and service adequacy; maintenance of a current software inventory.

Evidence Examined:	**Findings and observations:**	**Result/recommendation:**
	The DR accepts feedback regarding service, but there is no systematic solicitation of user feedback. Library maintains a current software inventory.	Investigate the development of distinct user group profiles that account for different needs, expectations, and use within each designated community.

5.1.1.1.6 The repository shall have procedures in place to monitor and receive notifications when software changes are needed.

Evidence: Audits of capacity versus actual usage; audits of observed error rates; audits of performance bottlenecks that limit ability to meet user community access requirements; documentation of technology watch assessments; documentation of software updates from vendors.

Evidence Examined:	**Findings and observations:**	**Result/recommendation:**
	Ad-hoc monitoring based on observed performance and user feedback.	Recommend that staff research these points regarding monitoring and notification, but we do not presently recommend that we implement any specific procedures.

5.1.1.1.7 The repository shall have procedures in place to evaluate when changes are needed to current software.

Evidence: Evaluation procedures in place; documented staff expertise in each software technology subsystem.

Evidence Examined:	Findings and observations:	Result/recommendation:
	No formal, scheduled evaluation procedures.	Those components that are managed in-house should be identified and polices and procedures developed and implemented to evaluate current and future software needs. Evaluation schedules should include reviews of hosted services for continuing performance and suitability.

5.1.1.1.8 The repository shall have procedures, commitment, and funding to replace software when evaluation indicates the need to do so.

Evidence: Statement of commitment to provide expected and contracted levels of service; evidence of ongoing financial assets set aside for software procurement; demonstration of cost savings through amortized cost of new system.

Evidence Examined:	Findings and observations:	Result/recommendation:
Ask Mike Taylor and Janet Crum	Ability to incorporate new technologies through funding commitments/cost reduction and operationally through verification of the capabilities of the new systems.	The library should develop financial and operational procedures and commitments for replacing software based on a regular, systematic review by repository staff.

	5.1.1.2 The repository shall have adequate hardware and software support for backup functionality sufficient for preserving the repository content and tracking repository functions.													
		Evidence: Documentation of what is being backed up and how often; audit log/inventory of backups; validation of completed backups; disaster recovery plan, policy and documentation; fire drills; testing of backups; support contracts for hardware and software for backup mechanisms; demonstrated preservation of system metadata such as access controls, location of replicas, audit trails, checksum values.											
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
				Hosted solution providers (AWS, CONTENTdm) perform backup procedures.					Create document defining how AWS (relationship/location of files in S3 and Glacier), CONTENTdm, EPrints, and NAU secure the data and system comprising the DR/IR. The current effort to amend and update the library's disaster preparedness and recovery must include procedures related to the digital repositories. Create document describing current METS schema (i.e. checksum values) and system information (i.e. file structure within AWS, CONTENTdm and EPrints).					

	5.1.1.3 The repository shall have effective mechanisms to detect bit corruption or loss.													
		Evidence: Documents that specify bit error detection and correction mechanisms used; risk analysis; error reports; threat analysis; periodic analysis of the integrity of repository holdings.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
AWS online documentation; per Christian Sarason at CONTENTdm				AWS performs file "self-healing" with bit corruption/loss has been detected. CONTENTdm does not perform regular verification of file integrity (i.e. they claim to be a presentation solution, but will sell their digital archive service). MD5 checksums are used with Cloudberry client for upload checking.					Recommend creating written documentation on our existing practices for managing file for reliability and durability. MD5 checksums should be used via download and independent verification with preservation metadata in CONTENTdm. Add to documentation referenced above and mention procedures for detecting, reporting, and repair corrupt/loss data.					

	5.1.1.3.1 The repository shall record and report to its administration all incidents of data corruption or loss, and steps shall be taken to repair/replace corrupt or lost data.													
		Evidence: Procedures related to reporting incidents to administrators; preservation metadata (e.g., PDI) records; comparison of error logs to reports to administration; escalation procedures related to data loss; tracking of sources of incidents; remediation actions taken to remove sources of incidents.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
AWS online documentation; per Christian Sarason at CONTENTdm				AWS provides documentation on their processes to detect and repair data corruption/loss, but do not send reports on incidents. CONTENTdm does report incidents of data loss when detected. The DR extracts and saves PDI information in its METS schema for internal/independent tracking and management purposes.					Recommend regularly (i.e. quarterly) scheduled exporting from CONTENTdm collection metadata into tab-delimited files for redundancy.					

5.1.1.4 The repository shall have a process to record and react to the availability of new security updates based on a risk-benefit assessment.

Evidence: Risk register (list of all patches available and risk documentation analysis); evidence of update processes (e.g., server update manager daemon); documentation related to the update installations.

Evidence Examined:	Findings and observations:	Result/recommendation:
AWS online documentation; per Christian Sarason at CONTENTdm	CONTENTdm updates are recorded on the User Support Center website. The hosted server updates are handled by OCLC. AWS and Cloudberry (3rd party) software update documentation is not readily available.	Create procedures for identifying and assessing risks and regularly evaluating hosted systems for risk handling.

5.1.1.5 The repository shall have defined processes for storage media and/or hardware change (e.g., refreshing, migration).

Evidence: Documentation of migration processes; policies related to hardware support, maintenance, and replacement; documentation of hardware manufacturer's expected support life cycles; policies related to migration of records to alternate hardware systems.

Evidence Examined:	Findings and observations:	Result/recommendation:
AWS online documentation; per Christian Sarason at CONTENTdm	DR moved to hosted storage solution (i.e. AWS) in Spring 2013 to mitigate continual hardware refreshment, maintenance, and replacement. CONTENTdm and OCLC observes the ISO-9001 certified operations practices include regular evaluation and refreshment of hardware, storage, and networking capabilities. They have redundant architecture in place that allows servers to be brought down/up as needed. Issues are communicated to customers for either planned outages, or in the instance of an unplanned outage.	Create procedures for regularly evaluating hosted systems for upgrade performance.

	5.1.1.6 The repository shall have identified and documented critical processes that affect its ability to comply with its mandatory responsibilities.													
		Evidence: Traceability matrix between processes and mandatory requirements.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
				We must recognize the changes in the broader technology environment, develop the necessary adjustments to the repository needs and requirements, and train staff on the appropriate changes.					The creation of the suite of documentation recommended throughout audit will result in identification and documentation of critical processes.					
	5.1.1.6.1 The repository shall have a documented change management process that identifies changes to critical processes that potentially affect the repository's ability to comply with its mandatory responsibilities.													
		Evidence: Documentation of change management process; assessment of risk associated with a process change; analysis of the expected impact of a process change; comparison of logs of actual changes to processes versus associated analyses of their impact and criticality.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
				Ad-hoc change response.					Recommend development of procedures for performing operational change analyses for the repositories. Process must recognize the changes in the broader technology environment, develop the necessary adjustments to the repository needs and requirements, and train staff on the appropriate changes.					

	5.1.1.6.2 The repository shall have a process for testing and evaluating the effect of changes to the repository's critical processes.													
		Evidence: Documented testing procedures; documentation of results from prior tests and proof of changes made as a result of tests; analysis of the impact of a process change.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
AWS online documentation; per Christian Sarason of CONTENTdm				CONTENTdm has multi-level, off-line testing of updates to its infrastructure environment. AWS procedures presumed to be based on Amazon's own critical commercial needs. AWS and CONTENTdm are both ISO 90001 certified.					Inquire as to how Eprints handles testing and evaluating changes to a repository's critical processes. Repositories must develop off-line testing procedures for any proposed changes to in-house repository operations.					
	5.1.2 The repository shall manage the number and location of copies of all digital objects.													
		Evidence: Random retrieval tests; validation of object existence for each registered location; validation of a registered location for each object on storage systems; provenance and fixity checking information; location register/log of digital objects compared to the expected number and location of copies of particular objects.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
per Todd Welch				Current procedures for fixity and integrity checking are accurate, but are performed on an ad-hoc basis.					Recommend creating written documentation on our existing practices for managing file for reliability and durability. MD5 checksums with Cloudberry and through download and independent verification with preservation metadata in CONTENTdm.					

	5.1.2.1 The repository shall have mechanisms in place to ensure any/multiple copies of digital objects are synchronized.													
		Evidence: Synchronization workflows; system analysis of how long it takes for copies to synchronize; procedures/documentation of synchronization processes.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
per Todd Welch									Recommend testing the durability of duplicate copies of master files in S3 and Glacier. Find utility that allows us to do this, but also independently verify with random retrieval of file from Glacier for md5 comparison.					

5.2 Security risk management			Notes
	5.2.1 The repository shall maintain a systematic analysis of security risk factors associated with data, systems, personnel, and physical plant.		
	Evidence: Repository employs the codes of practice found in the ISO 27000 series of standards system control list; risk, threat, or control analysis.		
Evidence Examined:	**Findings and observations:**	**Result/recommendation:**	
AWS online documentation; per Christian Sarason of CONTENTdm	AWS and CONTENTdm both conform to ISO 27000 series standards. In-house systems have not been deliberately analyzed for risk.	Create repository systems overview documents defining how AWS, CONTENTdm, EPrints, and NAU secure the data and system comprising the DR/IR. The documentation should include the protocols, policies, and procedures needed to maintain the repository.	
	5.2.2 The repository shall have implemented controls to adequately address each of the defined security risks.		
	Evidence: Repository employs the codes of practice found in the ISO 27000 series of standards; system control list; risk, threat, or control analyses; and addition of controls based on ongoing risk detection and assessment. Repository maintains ISO 17799 certification.		
Evidence Examined:	**Findings and observations:**	**Result/recommendation:**	
AWS online documentation; per Christian Sarason of CONTENTdm	AWS and CONTENTdm both conform to ISO 27000 series standards (including ISO 27002, formerly ISO 17799). In-house systems controls bear re-examining.	Create repository systems overview document as above; examine systems as documented to create a risk/threat analysis. Plan response for risk factors within in-house systems and practices.	

	5.2.3 The repository staff shall have delineated roles, responsibilities, and authorizations related to implementing changes within the system.													
		Evidence: Repository employs the codes of practice found in the ISO 27000 series of standards; organizational chart; system authorization documentation. Repository maintains ISO 17799 certification.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
AWS online documentation; per Christian Sarason of CONTENTdm				AWS and CONTENTdm both conform to ISO 27000 series standards (including ISO 27002, formerly ISO 17799). In-house roles are moderately well-defined.					Create repository systems overview document as above. Define staff roles in terms of security access and concerns (see SHERPA document).					
	5.2.4 The repository shall have suitable written disaster preparedness and recovery plan(s), including at least one off-site backup of all preserved information together with an offsite copy of the recovery plan(s).													
		Evidence: Repository employs the codes of practice found in the ISO 27000 series of standards; disaster and recovery plans; information about and proof of at least one off-site copy of preserved information; service continuity plan; documentation linking roles with activities; local geological, geographical, or meteorological data or threat assessments. Repository maintains ISO 17799 certification.												
Evidence Examined:				**Findings and observations:**					**Result/recommendation:**					
AWS online documentation; per Christian Sarason of CONTENTdm				AWS and CONTENTdm both conform to ISO 27000 series standards (including ISO 27002, formerly ISO 17799). Status of in-house systems in emergency management plan is undefined.					Create repository systems overview document as above. The current effort to amend and update the library's disaster preparedness and recovery must include procedures related to the digital repositories.					