

BS ISO 16363:2012



BSI Standards Publication

Space data and information transfer systems — Audit and certification of trustworthy digital repositories

bsi.

...making excellence a habit.
AVA **Documents**
Document Sharing Hub

National foreword

This British Standard is the UK implementation of ISO 16363:2012.

The UK participation in its preparation was entrusted to Technical Committee ACE/68/-/7, Space systems and operations - Space data and information transfer systems.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2012. Published by BSI Standards Limited 2012

ISBN 978 0 580 72840 2

ICS 49.140

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 29 February 2012.

Amendments issued since publication

Date	Text affected
------	---------------

INTERNATIONAL STANDARD

BS ISO 16363:2012

ISO
16363

First edition
2012-02-15

Space data and information transfer systems — Audit and certification of trustworthy digital repositories

*Systèmes de transfert des informations et données spatiales — Audit et
certification des référentiels numériques de confiance*



Reference number
ISO 16363:2012(E)
Documents
Document Sharing Hub
© ISO 2012



COPYRIGHT PROTECTED DOCUMENT

© ISO 2012

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 16363 was prepared by the Consultative Committee for Space Data Systems (CCSDS) (as CCSDS 652.0-M-1, September 2011) and was adopted (without modifications except those stated in Clause 2 of this International Standard) by Technical Committee ISO/TC 20, *Aircraft and space vehicles*, Subcommittee SC 13, *Space data and information transfer systems*.

Space data and information transfer systems — Audit and certification of trustworthy digital repositories

1 Scope

This International Standard defines a recommended practice for assessing the trustworthiness of digital repositories. It is applicable to the entire range of digital repositories. This International Standard can be used as a basis for certification.

The scope and field of application are furthermore detailed in subclauses 1.1 and 1.2 of the enclosed CCSDS publication.

2 Requirements

Requirements are the technical recommendations made in the following publication (reproduced on the following pages), which is adopted as an International Standard:

CCSDS 652.0-M-1, September 2011, *Audit and certification of trustworthy digital repositories*

For the purposes of international standardization, the modifications outlined below shall apply to the specific clauses and paragraphs of publication CCSDS 652.0-M-1.

Pages i to v

This part is information which is relevant to the CCSDS publication only.

Page 1-6

Add the following information to the reference indicated:

[1] Document CCSDS 650.0-B-1, January 2002, is equivalent to ISO 14721:2003.

Page B-1

Add the following information to the reference indicated:

[B5] Document CCSDS 661.0-B-1, September 2008, is equivalent to ISO 13527:2010.

[B6] Document CCSDS 644.0-B-3, June 2010, is equivalent to ISO 15889:2011.

[B7] Document CCSDS 647.1-B-1, June 2001, is equivalent to ISO 21961:2003.

3 Revision of publication CCSDS 652.0-M-1

It has been agreed with the Consultative Committee for Space Data Systems that Subcommittee ISO/TC 20/SC 13 will be consulted in the event of any revision or amendment of publication CCSDS 652.0-M-1. To this end, NASA will act as a liaison body between CCSDS and ISO.

(blank page)

Recommendation for Space Data System Practices

AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES

RECOMMENDED PRACTICE

CCSDS 652.0-M-1

MAGENTA BOOK
September 2011

(blank page)

AUTHORITY

Issue:	Recommended Practice, Issue 1
Date:	September 2011
Location:	Washington, DC, USA

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and represents the consensus technical agreement of the participating CCSDS Member Agencies. The procedure for review and authorization of CCSDS documents is detailed in the *Procedures Manual for the Consultative Committee for Space Data Systems*, and the record of Agency participation in the authorization of this document can be obtained from the CCSDS Secretariat at the address below.

This document is published and maintained by:

CCSDS Secretariat
Space Communications and Navigation Office, 7L70
Space Operations Mission Directorate
NASA Headquarters
Washington, DC 20546-0001, USA

STATEMENT OF INTENT

The Consultative Committee for Space Data Systems (CCSDS) is an organization officially established by the management of its members. The Committee meets periodically to address data systems problems that are common to all participants, and to formulate sound technical solutions to these problems. Inasmuch as participation in the CCSDS is completely voluntary, the results of Committee actions are termed **Recommendations** and are not in themselves considered binding on any Agency.

CCSDS Recommendations take two forms: **Recommended Standards** that are prescriptive and are the formal vehicles by which CCSDS Agencies create the standards that specify how elements of their space mission support infrastructure shall operate and interoperate with others; and **Recommended Practices** that are more descriptive in nature and are intended to provide general guidance about how to approach a particular problem associated with space mission support. This **Recommended Practice** is issued by, and represents the consensus of, the CCSDS members. Endorsement of this **Recommended Practice** is entirely voluntary and does not imply a commitment by any Agency or organization to implement its recommendations in a prescriptive sense.

No later than five years from its date of issuance, this **Recommended Practice** will be reviewed by the CCSDS to determine whether it should: (1) remain in effect without change; (2) be changed to reflect the impact of new technologies, new requirements, or new directions; or (3) be retired or canceled.

In those instances when a new version of a **Recommended Practice** is issued, existing CCSDS-related member Practices and implementations are not negated or deemed to be non-CCSDS compatible. It is the responsibility of each member to determine when such Practices or implementations are to be modified. Each member is, however, strongly encouraged to direct planning for its new Practices and implementations towards the later version of the Recommended Practice.

FOREWORD

This document is a technical Recommendation to use as the basis for providing audit and certification of the trustworthiness of digital repositories. It provides a detailed specification of criteria by which digital repositories shall be audited.

The OAIS Reference Model (reference [1]) contained a roadmap which included the need for a certification standard. The initial work was to be carried out outside CCSDS and then brought back into CCSDS to take into the standard.

In 2003, Research Libraries Group (RLG) and the National Archives and Records Administration (NARA) created a joint task force to specifically address digital repository certification. That task force published *Trustworthy Repositories Audit & Certification: Criteria and Checklist* (TRAC—reference [B3]), on which this Recommended Practice is based.

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Recommended Practice is therefore subject to CCSDS document management and change control procedures, which are defined in the *Procedures Manual for the Consultative Committee for Space Data Systems*. Current versions of CCSDS documents are maintained at the CCSDS Web site:

<http://www.ccsds.org/>

Questions relating to the contents or status of this document should be addressed to the CCSDS Secretariat at the address indicated on page i.

At time of publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

- Agenzia Spaziale Italiana (ASI)/Italy.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- China National Space Administration (CNSA)/People's Republic of China.
- Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (FSA)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.
- UK Space Agency/United Kingdom.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- China Satellite Launch and Tracking Control General, Beijing Institute of Tracking and Telecommunications Technology (CLTC/BITTT)/China.
- Chinese Academy of Sciences (CAS)/China.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- CSIR Satellite Applications Centre (CSIR)/Republic of South Africa.
- Danish National Space Center (DNSC)/Denmark.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Geo-Informatics and Space Technology Development Agency (GISTDA)/Thailand.
- Hellenic National Space Committee (HNSC)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- KFKI Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic and Atmospheric Administration (NOAA)/USA.
- National Space Agency of the Republic of Kazakhstan (NSARK)/Kazakhstan.
- National Space Organization (NSPO)/Chinese Taipei.
- Naval Center for Space Technology (NCST)/USA.
- Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.

AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES

- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 652.0-M-1	Audit and Certification of Trustworthy Digital Repositories, Recommended Practice, Issue 1	September 2011	Original issue

CONTENTS

<u>Section</u>	<u>Page</u>
1 INTRODUCTION	1-1
1.1 PURPOSE AND SCOPE.....	1-1
1.2 APPLICABILITY	1-1
1.3 RATIONALE.....	1-1
1.4 STRUCTURE OF THIS DOCUMENT.....	1-2
1.5 DEFINITIONS.....	1-3
1.6 CONFORMANCE.....	1-6
1.7 REFERENCES	1-6
2 OVERVIEW OF AUDIT AND CERTIFICATION CRITERIA	2-1
2.1 A TRUSTWORTHY DIGITAL REPOSITORY.....	2-1
2.2 EVIDENCE.....	2-1
2.3 RELEVANT STANDARDS, BEST PRACTICES, AND CONTROLS	2-1
3 ORGANIZATIONAL INFRASTRUCTURE	3-1
3.1 GOVERNANCE AND ORGANIZATIONAL VIABILITY	3-1
3.2 ORGANIZATIONAL STRUCTURE AND STAFFING	3-3
3.3 PROCEDURAL ACCOUNTABILITY AND PRESERVATION POLICY FRAMEWORK	3-5
3.4 FINANCIAL SUSTAINABILITY.....	3-10
3.5 CONTRACTS, LICENSES, AND LIABILITIES	3-11
4 DIGITAL OBJECT MANAGEMENT	4-1
4.1 INGEST: ACQUISITION OF CONTENT	4-1
4.2 INGEST: CREATION OF THE AIP	4-6
4.3 PRESERVATION PLANNING	4-16
4.4 AIP PRESERVATION	4-19
4.5 INFORMATION MANAGEMENT.....	4-23
4.6 ACCESS MANAGEMENT	4-24
5 INFRASTRUCTURE AND SECURITY RISK MANAGEMENT	5-1
5.1 TECHNICAL INFRASTRUCTURE RISK MANAGEMENT.....	5-1
5.2 SECURITY RISK MANAGEMENT	5-12
ANNEX A SECURITY CONSIDERATIONS (NORMATIVE)	A-1
ANNEX B REFERENCES (INFORMATIVE)	B-1

(blank page)

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:
 - covers Organizational Infrastructure;
 - covers Digital Object Management;
 - 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.

3 ORGANIZATIONAL INFRASTRUCTURE

3.1 GOVERNANCE AND 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.

Supporting Text

This is necessary in order to ensure commitment to preservation, retention, management and access at the repository's highest administrative level.

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

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.

Discussion

The repository's or its parent organization's mission statement should explicitly address preservation. If preservation is not among the primary purposes of an organization that houses a digital repository then preservation may not be essential to the organization's mission. In some instances a repository pursues its preservation mission as an outgrowth of the larger goals of an organization in which it is housed, such as a university or a government agency, and its narrower mission may be formalized through policies explicitly adopted and approved by the larger organization. Government agencies and other organizations may have legal mandates that require they preserve materials, in which case these mandates can be substituted for mission statements, as they define the purpose of the organization. Mission statements should be kept up to date and continue to reflect the common goals and practices for preservation.

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.

Supporting Text

This is necessary in order to help the repository make administrative decisions, shape policies, and allocate resources in order to successfully preserve its holdings.

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

Preservation Strategic Plan; meeting minutes; documentation of administrative decisions which have been made.

Discussion

The strategic plan should be based on the organization's established mission, and on its defined values, vision and goals. Strategic plans typically cover a particular finite time period, normally in the 3-5 year range.

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.**Supporting Text**

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

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

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

Discussion

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

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.**Supporting Text**

This is necessary in order to ensure that the repository can recognize when it is necessary to execute those plans.

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

Administrative policies, procedures, protocols, requirements; budgets and financial analysis documents; fiscal calendars; business plan(s); any evidence of active monitoring and preparedness.

Discussion

The management of a repository should have formal procedures in place to periodically check on the viability of the repository. This periodic check should be used to determine if, or when, to execute the repository's formal succession plan, contingency plans, and/or escrow arrangements.

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.

Supporting Text

This is necessary in order that the repository has guidance on acquisition of digital content it will preserve, retain, manage and provide access to.

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

Collection policy and supporting documents; Preservation Policy, mission, goals and vision of the repository.

Discussion

The collection policy can be used to understand what the repository holds, what it does not hold, and why. The collection policy supports the broader mission of the repository. Without such a policy the repository is likely to collect in a haphazard manner, or store large amounts of low-value digital content. The collection policy helps the organization to identify what digital content it will and will not accept for ingestion. In an organization with a broader mission than preservation of digital content the collection policy helps to define the role of the repository within the larger organizational context.

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.

Discussion

Staffing of the repository should be by personnel with the required training and skills to carry out the activities of the repository. The repository should be able to document through