



DPC: 23/30477110 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 19 December 2023

Origin: International

Latest date for receipt of comments: 11 February 2024

Project No. 2023/01562

Responsible committee: ACE/68 Space systems and operations

Interested committees:

Title: Draft BS ISO 16363 Draft Space data and information transfer systems. Audit and certification of trustworthy digital repositories.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 11 February 2024

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

DRAFT INTERNATIONAL STANDARD

ISO/DIS 16363

ISO/TC 20/SC 13

Secretariat: ANSI

Voting begins on:
2023-12-19

Voting terminates on:
2024-03-12

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

ICS: 49.140

This document is circulated as received from the committee secretariat.

FAST TRACK PROCEDURE

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.



Reference number
ISO/DIS 16363:2023(E)
Documents
Document Sharing Hub
© ISO 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

AUTHORITY

Issue:	Pink Book, Issue 1.1
Date:	November 2021
Location:	Not Applicable

(WHEN THIS RECOMMENDED PRACTICE IS FINALIZED, IT WILL CONTAIN THE FOLLOWING STATEMENT OF AUTHORITY:)

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 *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4), and the record of Agency participation in the authorization of this document can be obtained from the CCSDS Secretariat at the email address below.

This document is published and maintained by:

CCSDS Secretariat
National Aeronautics and Space Administration
Washington, DC, USA
Email: secretariat@mailman.ccsds.org

STATEMENT OF INTENT

(WHEN THIS RECOMMENDED PRACTICE IS FINALIZED, IT WILL CONTAIN THE FOLLOWING 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.

AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES

FOREWORD

This document is a draft 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.

Its ‘White Book’ status indicates that its contents are not stable, and several iterations resulting in substantial technical changes are likely to occur before it is considered to be sufficiently mature to be released for review by the CCSDS Agencies.

Implementers are cautioned **not** to fabricate any final equipment in accordance with this document’s technical content.

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 the 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 Standard is therefore subject to CCSDS document management and change control procedures, which are defined in the *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-4). 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 sent to the CCSDS Secretariat at the email 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 (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 Science Policy Office (BELSPO)/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.
- China Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish National Space Center (DNSC)/Denmark.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- Electronics and Telecommunications Research Institute (ETRI)/Korea.
- 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.
- Hellenic Space Agency (HSA)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- Mohammed Bin Rashid Space Centre (MBRSC)/United Arab Emirates.
- 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.
- Netherlands Space Office (NSO)/The Netherlands.
- Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
- South African National Space Agency (SANSA)/Republic of South Africa.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- Swiss Space Office (SSO)/Switzerland.

AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES

- United States Geological Survey (USGS)/USA.

PREFACE

This document is a draft CCSDS Recommended Practice. Its ‘Pink Book’ status indicates that the CCSDS believes the document to be technically mature and has released it for formal review by appropriate technical organizations. As such, its technical contents are not stable, and several iterations of it may occur in response to comments received during the review process.

Implementers are cautioned **not** to fabricate any final equipment in accordance with this document’s technical content.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES

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
CCSDS 652.0-P-1.1	Audit and Certification of Trustworthy Digital Repositories, Draft Recommended Practice, Issue 1.1	November 2021	Current draft update

NOTE – Changes from the original issue are indicated with markup and change bars in the right margin.

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	3-4
3.3 PROCEDURAL ACCOUNTABILITY AND PRESERVATION POLICY FRAMEWORK	3-5
3.4 FINANCIAL SUSTAINABILITY	3-11
3.5 CONTRACTS, LICENSES, AND LIABILITIES	3-13
4 DIGITAL OBJECT MANAGEMENT	4-1
4.1 INGEST: ACQUISITION OF CONTENT	4-1
4.2 INGEST: CREATION OF THE AIP	4-7
4.3 PRESERVATION PLANNING	4-17
4.4 AIP PRESERVATION	4-21
4.5 INFORMATION MANAGEMENT	4-25
4.6 ACCESS MANAGEMENT	4-26
5 INFRASTRUCTURE AND SECURITY RISK MANAGEMENT	5-1
5.1 TECHNICAL INFRASTRUCTURE RISK MANAGEMENT	5-1
5.2 SECURITY RISK MANAGEMENT	5-13
ANNEX A SECURITY, SANA, AND PATENT CONSIDERATIONS (INFORMATIVE)	A-1
ANNEX B REFERENCES (INFORMATIVE)	B-1

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.

AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES

- Sections 3 to 5 provide the normative metrics against which a digital repository may be judged. These sections provide metrics grouped as follows:
 - section 3 covers Organizational Infrastructure;
 - section 4 covers Digital Object Management;
 - section 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
CCSDS	Consultative Committee for Space Data Systems
DEDSL	Data Entity Specification Language
DIP	Dissemination Information Package
FITS	Flexible Image Transport System
GIS	Geographic Information System
ISO	International Organization for Standardization
OAIS	Open Archival Information System
PDI	Preservation Description Information
SIP	Submission Information Package
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 user 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.

NOTE – The relationship between the terms below 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.

1.5.2.1 Glossary

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

Access Policy: Documented 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, members of the Designated Community, 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 documented 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.

AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES

Preservation Policy: Documented 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 documented 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 documented 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 documented 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 user communities. A repository may have a different Designated Community for different collections of information and so a repository may be said to have multiple Designated Communities.
- The term 'written statement' or 'documented statement' is meant to make it clear that verbal statements are not adequate.

AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES

- 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.

NOTE – It is assumed that a formal system development life cycle was used in the development of the repository system and that a set of well-defined documents exist that could be used as evidence. The names of documents that might be used in ‘Examples of Ways the Repository Can Demonstrate It Is Meeting This Requirement’ text are intended to be easily mappable to whatever documentation nomenclature that the repository uses.

- Discussion: clarifications about the intent of the metric.

1.6 CONFORMANCE

An archive that conforms to this Recommended Practice shall have documented its design and requirements, and shall have satisfied an auditor on each of the Requirements, which are referred to as metrics below. Because the requirements cannot specify every possible detail, the judgement of the auditor will come into play.. The supporting organization and practice of auditing will lead to the creation of auditors’ guidelines, as described in the Requirements for Bodies Conducting Audit and Certification of Candidate Trustworthy Digital Repositories (reference [2]).

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.

AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES

- [1] *Reference Model for an Open Archival Information System (OAIS)*. Issue 2. Recommendation for Space Data System Practices (Magenta Book), CCSDS 650.0-M-2. Washington, D.C.: CCSDS, June 2012 [Also published as ISO 14721:2012] or later version.
- [2] *Requirements for Bodies Providing Audit and Certification of Candidate Trustworthy Digital Repositories*. Issue 2. Recommendation for Space Data System Practices (Magenta Book), CCSDS 652.1-M-2. Washington, D.C.: CCSDS, March 2014 [Also published as ISO 16919:2014] or later version.

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 (where allowed)—that is, 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,

AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES

were not specifically developed to gauge the trustworthiness of organizations operating digital repositories.

- Similarly, ISO 17799:2005, Information Technology—Security Techniques—Code of Practice for Information Security Management (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, Information and Documentation—Records Management—Part 1: General (reference [B11]), and ISO 15489-2:2001, Information and Documentation—Records Management—Part 2: Guidelines (reference [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, the Open Archival Information System Reference Model (reference [1]), 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 or the repository can no longer commit to the long-term preservation of the specific digital objects.

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 information 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. The length of time of future guaranteed funding will be a factor in determining the risk to be mitigated.

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.

AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES

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. The checks could involve comparing the time it would take to hand over holdings to a successor with the time to the end of the current funding cycle and any potential gaps with the next funding cycle.

In order to reduce the time it would take to hand over holdings it might be practical, for example, to have copies of all AIPs and Access Aids in a system independent format (i.e., not have to rely on export functions of existing systems) so that the information could be transferred to a successor repository on very short notice.

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 development plans, organizational charts, job descriptions, and related policies and procedures that the repository is defining and maintaining the skills and roles that are required for the sustained operation of the repository.

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

Supporting Text

This is necessary in order to ensure that the repository can complete all tasks associated with the long-term preservation and management of the data objects.

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

A staffing plan; competency definitions; job descriptions; staff professional development plans; certificates of training and accreditation; plus evidence that the repository reviews and maintains these documents as requirements evolve.

Discussion

Preservation depends upon a range of activities from maintaining hardware and software to migrating content and storage media to negotiating intellectual property rights agreements. In order to ensure long-term sustainability, a repository must be aware of all required activities and demonstrate that it can successfully complete them. The repository can achieve these aims by, for example, identifying the competencies and skill sets required to carry out its activities over time—e.g., archival training, technical skills, and legal expertise.

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

Supporting Text

This is necessary in order to ensure repository staffing levels are adequate for preserving the digital content and providing a secure, quality repository.

AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES

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

Organizational charts; definitions of roles and responsibilities; comparison of staffing levels to industry benchmarks and standards.

Discussion

The repository should determine the appropriate number and level of staff that corresponds to requirements and commitments. The repository should also demonstrate how it evaluates staff effectiveness and suitability to support its functions and services.

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

This is necessary to ensure that staff skill sets evolve as the repository technology and preservation procedures change.

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

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, individual training plans (with evidence of periodic review and any updates), and training logs.

Discussion

Technology and general practices for digital preservation will continue to change, as will the requirements of its Designated Community, so the repository must ensure that its staff's skill sets evolve. Ideally the repository will meet this requirement through a lifelong learning approach to developing and retaining staff.

3.3 PROCEDURAL ACCOUNTABILITY AND PRESERVATION POLICY FRAMEWORK

Documentation assures stakeholders (consumers, producers, and contributors of digital content) that the repository is meeting its requirements and fully performing its role as a trustworthy digital repository. A repository must create documentation that reflects its Mission Statement and Strategic Plan and captures its normal activities. This entails documenting all repository processes, decision-making, and goal setting. Documentation is provided so that the activities of the repository will be understood by stakeholders and management. It ensures that repository policies and procedures are carried out in approved, consistent ways, resulting in long-term preservation and access to digital content in its care.