International Standard

ISO 16363

Second edition

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

PROOF/ÉPREUVE

Reference number
ISO 16363:2025(en)

COPYRIGHT PROTECTED DOCUMENT

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

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by the Consultative Committee for Space Data Systems (CCSDS) (as CCSDS 652.0-P-1.1, November 2021) and drafted in accordance with its editorial rules. It was assigned to Technical Committee ISO/TC 20, *Aircraft and space vehicles*, Subcommittee SC 13, *Space data and information transfer systems* and adopted under the "fast-track procedure".

This second edition cancels and replaces the first edition (ISO 16363:2012), which has been technically revised.

The main changes are as follows:

— updates to ensure consistency with updated ISO 14721, e.g. add mentions of "Preservation Objectives" in section 4.1.1.4 and 4.1.1.5, and added new 4.3.5;

— clarifications added to "Discussions" in several sections;

— added section 3.3.3 for better consistency with ISO 14721;

— changed "written" to "documented" in many metrics;

— changed "metadata" to "information" in many metrics;

— clarify Risk Management in section 5.1.1.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

CONTENTS

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, extends and clarifies TRAC in order to produce an ISO standard which can be used in an ISO audit and certification process.

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:

  • 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.

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.

– 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.

[1] *Reference Model for an Open Archival Information System (OAIS)*. Issue 3. Recommendation for Space Data System Practices (Magenta Book), CCSDS 650.0-M-3. Washington, D.C.: CCSDS, December 2024 [to be published as ISO 14721:2025[1]] or later version.

[2] *Requirements for Bodies Providing Audit and Certification of Candidate Trustworthy Digital Repositories*. Issue 3. Recommendation for Space Data System Practices (Magenta Book), CCSDS 652.1-M-3. Washington, D.C.: CCSDS, December 2024 [to be published as ISO 16919:2025[1]] or later version.

NOTE – Informative references are listed in annex B.

[1] Issue year is surmized.

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,

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.