BS ISO 16363:2025

BSI Standards Publication

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

Documents
Document Sharing Hub

Full document details: BS ISO 16363:2025

National foreword

This British Standard is the UK implementation of ISO 16363:2025. It supersedes BS ISO 16363:2012, which is withdrawn.

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

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

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 27846 0

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 31 March 2025.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO 16363:2025

International Standard

ISO 16363

Second edition
2025-03

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 16363:2025(en)

© ISO 2025

Documents
Document Sharing Hub

Full document details: BS ISO 16363:2025

COPYRIGHT PROTECTED DOCUMENT

© ISO 2025

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

Documents
Document Sharing Hub
Full document details: BS ISO 16363:2025

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.

© ISO 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 16363:2025

CONTENTS

Section Page

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 3-12
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 INFORMATIVE REFERENCES (INFORMATIVE) B-1

© ISO 2025 – All rights reserved

AVA Documents Document Sharing Hub

Full document details: BS ISO 16363:2025

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.

© ISO 2025 – All rights reserved

AVA Documents Document Sharing Hub

Full document details: BS ISO 16363:2025

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

© ISO 2025 – All rights reserved

Documents Document Sharing Hub

Full document details: BS ISO 16363:2025

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.

© ISO 2025 – All rights reserved

AVA Documents Document Sharing Hub

Full document details: BS ISO 16363:2025

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.

© ISO 2025 – All rights reserved

Documents Document Sharing Hub

Full document details: BS ISO 16363:2025

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.

© ISO 2025 – All rights reserved

AVA Documents Document Sharing Hub

Full document details: BS ISO 16363:2025

– 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.

© ISO 2025 – All rights reserved

AVA Documents Document Sharing Hub

Full document details: BS ISO 16363:2025

[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.

© ISO 2025 – All rights reserved

Documents Document Sharing Hub

Full document details: BS ISO 16363:2025

© ISO 2025 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 16363:2025

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,

© ISO 2025 – All rights reserved

Document Sharing Hub

Full document details: BS ISO 16363:2025

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.

© ISO 2025 – All rights reserved

Documents Document Sharing Hub

Full document details: BS ISO 16363:2025

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.

© ISO 2025 – All rights reserved

AVA Documents Document Sharing Hub

Full document details: BS ISO 16363:2025

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.

© ISO 2025 – All rights reserved

Documents Document Sharing Hub

Full document details: BS ISO 16363:2025

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.

© ISO 2025 – All rights reserved

AVA Documents Document Sharing Hub

Full document details: BS ISO 16363:2025

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—for example, 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.

© ISO 2025 – All rights reserved

Documents Document Sharing Hub

Full document details: BS ISO 16363:2025

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. Certification, the clearest indicator of a repository's sound and standards-based practice, is facilitated by procedural accountability and documentation.

© ISO 2025 – All rights reserved

AVA Documents Document Sharing Hub

Full document details: BS ISO 16363:2025

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

Supporting Text

This is necessary in order that it is possible to test that the repository meets the needs of its Designated Community.

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

A written definition of the Designated Community.

Discussion

The Designated Community is defined as 'an identified group of potential Consumers who should be able to understand a particular set of information in ways exemplified by the Preservation Objectives. The Designated Community (reference [1]) may be composed of multiple user communities. A Designated Community is defined by the archive and this definition may change/evolve over time' (OAIS Glossary, reference [1]). In addition to and associated with a definition of the Designated Community for each AIP (or class of AIPs), Preservation Objectives will be defined for each AIP (or class of AIPs).

General Public versus Designated Community

The OAIS Reference Model, and this standard, do not require repositories to limit their Consumers to members of their Designated Communities. However, many repositories have as part of their mission/mandate to serve the general public. In other words, the repository must disseminate any information that the Consumer is allowed to access without violating any restrictions on the release of the requested information. Some repositories have raised concerns about the tension between their requirements to serve the general public and the OAIS requirement to serve the repository's Designated Community(ies).

The purposes for designating these two different roles, the Designated Community and the general public, do have some overlap, but they also have some substantive differences. Indicating that a repository serves the general public means that anyone (with a few exceptions) can be a Consumer of the OAIS' information. The repository assigns a Designated Community for each AIP or group of related AIPs. The repository then must ensure that the AIPs remain Independently Understandable (reference [1]) to the relevant Designated Community.

© ISO 2025 – All rights reserved

Documents Document Sharing Hub

Full document details: BS ISO 16363:2025

Designated Communities serve a distinct purpose related to the Long Term Preservation of the information held by the repository. Long Term Preservation is, "[t]he act of maintaining information, Independently Understandable by a Designated Community, and with evidence supporting its Authenticity, over the Long Term." One of the mandatory responsibilities of an OAIS is to ensure that the information it holds is Independently Understandable by the Designated Community. The OAIS must periodically assess whether or not the information held for a specific Designated Community is still Independently Understandable by that Designated Community using their current Knowledge Base (reference [1]). If it is not, the OAIS must add additional Representation Information or PDI (reference [1]) to make it so. If a repository collects information across many topics/domains, it may need to have multiple Designated Communities for the different topics/domains.

Under the OAIS Reference Model, and this standard, an OAIS does not have to ensure that its holdings are Independently Understandable to any Consumer outside its Designated Community(ies), though it may choose to try. In practical terms ensuring its holdings are and remain Independently Understandable to the general public would be a nearly impossible task. Consider, for example, trying to maintain enough Representation Information and PDI to make Einstein's Theory of General Relativity Independently Understandable to a 6-year-old who reads only their native language which is different from the language of Einstein's work. While many repositories will say they serve the general public, there are usually unwritten limits to the types of services the repository provides. By contrast, an OAIS must only ensure that the information it provides remains Independently Understandable to the relevant Designated Community through time.

Examples of Designated Community definitions include:

- General English-reading public educated to high school and above, with access to a Web Browser (HTML 4.0 capable).
- For Geographic Information System (GIS) data: GIS researchers—undergraduates and above—having an understanding of the concepts of Geographic data and having access to current (2005, USA) GIS tools/computer software, for example, ArcInfo (2005).
- Astronomer (undergraduate and above) with access to Flexible Image Transport System (FITS) software such as FITSIO, familiar with astronomical spectrographic instruments.
- Student of Middle English (a form of the English language spoken after the Norman conquest (1066) until the late 15th century) with an understanding of Text Encoding Initiative (TEI) encoding and access to an XML rendering environment.
    - Variant 1: Cannot understand TEI;
    - Variant 2: Cannot understand TEI and no access to XML rendering environment;
    - Variant 3: No understanding of Middle English but does understand TEI and XML.

© ISO 2025 – All rights reserved

AVA Documents Document Sharing Hub

Full document details: BS ISO 16363:2025

– The repository has defined the external parties, and its assets, owners, and uses. Two groups: the publishers of scholarly journals and their readers, each of whom have different rights to access material and different services offered to them.

Some repositories may call themselves, for example, a 'dark archive', an archive that has a policy not to allow consumers to get access to its contents for a certain period of time, but they would nevertheless need a Designated Community.

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

Supporting Text

This is necessary in order to ensure that the repository can fulfill that part of its mission related to preservation.

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

Preservation Policies; Repository Mission Statement.

Discussion

Repository policies show how the repository fulfills the requirements of the repository's Preservation Strategic Plan. For example, a Preservation Strategic Plan may contain a requirement that the repository 'comply with current preferred preservation standards'. The preservation policy might then require that the repository 'monitor current preservation standards and ensure repository compliance with the preferred preservation standards'. In another example the repository may be required by the strategic plan to keep its data understandable by the Designated Communities for the repository's AIPs. The preservation policy might then include information about the expected level of understandability by the repository's Designated Community for each Archival Information Package, as exemplified by the associated Preservation Objectives.

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

Supporting Text

This is necessary in order that the repository has up-to-date, complete policies and procedures in place that reflect the current requirements and practices of its community(ies) for preservation.

© ISO 2025 – All rights reserved

AVA Documents Document Sharing Hub

Full document details: BS ISO 16363:2025

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

Current and past written documentation in the form of Preservation Policies, Preservation Strategic Plans and Preservation Implementation Plans, procedures, protocols, and workflows; specifications of review cycles for documentation; documentation detailing reviews, surveys and feedback. If documentation is embedded in system logic, functionality should demonstrate the implementation of policies and procedures.

Discussion

Preservation Policies capture organizational commitments and intents for staffing, security and other preservation-related concerns. Preservation Implementation Plans address preservation activities and practices such as transfer, submission, quality control, storage management, information management, and access and rights management. The repository may find it beneficial to maintain all versions of the preservation policies (e.g., outdated versions are clearly identified and maintained in some organized way) in order to document the results of monitoring for new developments, showing the repository's responsiveness to prevailing standards and practice, emerging requirements, and standards that are specific to the domain, if appropriate, and similar developments. Qualified staff and peers are an important part of the review process, as they help to update and expand these documents. The policies should be understandable by the repository staff in order for them to carry out their work. Preservation Policies and procedures must be demonstrated to be understandable and implementable. The staff should be familiar with the Preservation Policies and have a mechanism to contribute to the review of them.

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

Supporting Text

This is necessary in order to provide an 'audit trail' through which stakeholders can identify and trace decisions made by the repository.

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

Capital equipment inventories; documentation of the acquisition, implementation, update, and retirement of critical repository software and hardware; file retention and disposal schedules and policies, copies of earlier versions of policies and procedures; minutes of meetings.

Discussion

This documentation may include decisions about the organizational and technical infrastructure. Documentation of or interviews with appropriate staff who can explain repository practices and workflow should be available.

© ISO 2025 – All rights reserved

AVA Documents Document Sharing Hub

Full document details: BS ISO 16363:2025

3.3.4 The repository shall commit to transparency and accountability in all actions supporting the operation and management of the repository that affect the preservation of digital content over time.

Supporting Text

This is necessary because transparency, in the sense of being available to anyone who is authorized to know. This could include everybody, but may be restricted, for example by legal, commercial, or security concerns. Transparency is the best assurance that the repository operates in accordance with accepted standards and practices.

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

Reports, including results, of financial and technical audits and certifications; disclosure of governance documents, independent program reviews, and contracts and agreements with providers of funding and critical services.

Discussion

If the repository uses software to capture information about its history, it should be able to demonstrate these tracking tools. Where appropriate, the history is linked to relevant preservation strategies and describes potential effects on preserving digital content. This requirement does not mean that the organization must make information which would make it vulnerable to competitors available, but rather that the organization commits to disclosing its methods for preserving digital content at least to the Designated Community or other appropriate stakeholder in order to demonstrate that it is meeting all current preservation requirements.

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

Supporting Text

This is necessary in order to provide documentation that it has developed or adopted/adapted appropriate measures for ensuring the integrity of its holding.

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

Written definition or specification of the repository's integrity measures (for example, computed checksum or hash value); documentation of the procedures and mechanisms for monitoring integrity measurements and for responding to results of integrity measurements that indicate digital content is at risk; an audit process for collecting, tracking, and presenting integrity measurements; Preservation Policy and workflow documentation.

© ISO 2025 – All rights reserved

Documents Document Sharing Hub

Full document details: BS ISO 16363:2025