INTERNATIONAL STANDARD

ISO 14641-1

First edition
2012-02-01

Electronic archiving —

Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation

Archivage électronique — Partie 1: Spécifications relatives à la conception et au fonctionnement d'un système d'informations pour la conservation d'informations électroniques

Reference number
ISO 14641-1:2012(E)

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

ISO 14641-1 was prepared by Technical Committee ISO/TC 171, *Document management applications*, Subcommittee SC 3, *General issues*.

ISO 14641 consists of the following parts, under the general title *Electronic archiving*:

— *Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation*

Future parts will address trusted content, data-level-controls and the testability of document integrity and authenticity control elements within document management systems.

Introduction

Electronic documents are an essential part of everyday business, whether the sources are incoming communications or output from organizations. It is important that electronic documents be stored appropriately, either fully or in part, in secure information systems designed for operations and archiving, in order to meet business, legal or regulatory requirements.

The objectives of secure information systems are to resolve organizational issues such as:

a) optimization of long-term electronic document preservation, archiving and integrity;

b) provision of information search facilities;

c) ensuring ease of access and use of electronic documents.

This part of ISO 14641 is intended to provide a reference framework for organizations. It describes the methods and techniques to be used for the implementation of an electronic information system for managing documents within an archive. In conjunction with related archival policies of organizations, it describes criteria for system design and specifications for operational processes.

These specifications are intended to ensure that all documents to be managed by the information system are captured, stored, retrieved and accessed in a way that guarantees that the archived document is an authentic rendition of the original document for the duration of preservation. An authentic rendition means that the rendered document corresponds to the source document as it was at the time of input in the information system in respect of criteria of fidelity and integrity, and that this state is maintained for the duration of preservation.

This part of ISO 14641 takes into account the use of three possible archiving media: physical WORM, logical WORM and rewritable media. Archival integrity is ensured on physical and logical WORM media by the inherent properties of WORM solutions. On rewritable media, integrity is ensured using encryption-like techniques, in particular with checksum calculation or hash function, date and time stamp or digital signature. In all cases, it is necessary to comply with related procedures.

Depending on the types of documents to be archived, other specialized standards can be relevant and used to complement the recommendations in this part of ISO 14641.

This part of ISO 14641 provides a specific and complementary definition of issues addressed in other standards or specifications concerning the management of electronic information. Its content is intended to address execution issues raised in several other documents. These include:

— ISO/TR 15801, *Document management — Information stored electronically — Recommendations for trustworthiness and reliability*,

— ISO 15489 (all parts), *Information and documentation — Records management*,

— MoReq2, *Model Requirements for the Management of Electronic Records*,

which detail specifications for organizing and controlling the lifecycle of archived information for purposes of evidence and operational history; and

— ISO 14721, *Space data and information transfer systems — Open archival information system — Reference model*,

which describes the characteristics of an open system for the preservation of digital data.

Annexes A, B and C are informative and complementary.

Electronic archiving —

Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation

1 Scope

This part of ISO 14641 provides a set of technical specifications and organizational policies to be implemented for the capture, storage and access of electronic documents. This ensures legibility, integrity and traceability of the documents for the duration of their preservation.

This part of ISO 14641 is applicable to electronic documents resulting from:

— the scanning of original paper or microform documents;

— the conversion of analogue audio or video content;

— the “native” creation by an information system application; or

— other sources that create digital content such as two- or three- dimensional maps, drawings or designs, digital audio/video, and digital medical images.

This part of ISO 14641 is not applicable to information systems in which users have the ability to substitute or alter documents after capture.

This part of ISO 14641 is intended for the following users.

a) Organizations implementing information systems in which:

   1) electronic documents created from scan captures are kept in an environment that ensures fidelity with regard to the original and long-term preservation;

   2) digitally born documents are kept in an environment that ensures the content integrity of the information and document legibility;

   3) traceability is ensured for all operations relating to the electronic documents.

b) Organizations providing information technology services and software publishers seeking to develop information systems that ensure the fidelity and integrity of electronic documents.

c) Organizations providing third-party document archiving services.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 2859 (all parts), *Sampling procedures for inspection by attributes*

ISO 8601, *Data elements and interchange formats — Information interchange — Representation of dates and times*

ISO/TR 12033, *Document management — Electronic imaging — Guidance for the selection of document image compression methods*

ISO 12653-1, *Electronic imaging — Test target for the black-and-white scanning of office documents — Part 1: Characteristics*

ISO 12653-2, *Electronic imaging — Test target for the black-and-white scanning of office documents — Part 2: Method of use*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12653-1 and ISO 12653-2 and the following apply.

3.1
access
processes of retrieving and displaying (playing) electronic documents for operational, evidential or historical purposes

3.2
archive(s)
set of documents produced or received, whatever their date, format or storage media, by any individual, organization, public or private service, in the course of their activity

3.3
archival policy
legal, functional, operational, technical and security requirements of an internal or external information system

NOTE Annexes A and B give principles of an archival policy and of a declaration of archival practices.

3.4
archive lifecycle log
log which records audit trail data related to the document lifecycle archiving process

3.5
archive restitution
return and transfer of archived documents to their originator, or to a duly appointed person or organization

3.6
archival system profile
set of properties that applies to a class of archives that share common characteristics in terms of confidentiality, retention and disposal schedules, and access rights (e.g. create, read, modify, delete)

3.7
ACU
attestation creation unit
hardware and/or software devices for the delivery of electronic attestations

NOTE Attestations include a unit identifier and the related archival service identifier.

3.8
audiovisual
communication techniques combining sound and image

3.9
audit trail
aggregate of the information necessary to provide a historical record of all significant events associated with stored information and the information system

3.10
data
digital form of information which can be accessed, read and/or processed

3.11
date and time stamp
sequence of characters denoting the date and/or time at which a certain event occurred

3.12
deposit
set of documents sharing the same archival system profile

3.13
digital archival
set of actions aiming to identify, capture, classify, preserve, retrieve, display and provide access to documents for informational or historical purposes, or for the duration required to meet legal obligations

3.14
digital document
digital representation of content that is stored and managed electronically

NOTE Association of content, logical structure and display attributes, retrievable by a device capable of rendering a human-readable (or machine-readable) object. A document can be digitally born (creation) at source or converted from an analogue document.

3.15
digital fingerprint
bit sequence generated from a digital document using an algorithm that uniquely identifies the original document

NOTE Any digital document modification will produce a different fingerprint.

3.16
digital seal
method for ensuring the integrity of a document including hash functions, digital signatures and, optionally, a date and time stamp

3.17
digital signature
data which, when appended to a digital document, enable the user of the document to authenticate its origin and integrity

3.18
digitization
conversion of an analogue document (paper, microform, film, analogue audio or audiovisual tapes) to digital format for the purpose of preservation or processing

3.19
digitized document
result of digitization of information initially stored on physical media (paper, microform, and film, analogue audio or audiovisual tapes)

3.20
document fidelity
property of an archived document which renders all the information contained in the original source document

NOTE This notion is applicable to any change of form, including digitization or format conversion.

3.21
durability
attribute of a document which remains readable during its entire lifecycle

3.22
electronic information system
system designed to receive, preserve, access and transfer archives in an electronic form

3.23
electronic attestation
information produced to provide evidence that an action or an electronic transaction has occurred

3.24
events log
log which records audit trail data related to the system operations

3.25
format conversion
operation converting a digital document to a different electronic format

NOTE This operation preserves the fidelity of the document.

3.26
hash function
mathematical algorithm used for turning some kinds of data into a relatively small integer

3.27
integrity
attribute of a document whose content is completed and unaltered

3.28
legibility
attribute of an archived document which allows access to all the information it contains

NOTE This could be facilitated by certain metadata associated with the document.

3.29
lossy compression
compression algorithm which loses some of the original information during compression

NOTE The resulting decompressed object is only an approximation of the original.

3.30
media migration
act of transferring a document from one medium to another, particularly with regard to managing media obsolescence

3.31
metadata
data describing the context, content and structure of a document and their management over time

3.32
replication
process which consists of copying information between redundant resources, notably software or hardware components, to improve reliability, fault-tolerance or accessibility

3.33
time source
internal or external component of an information system providing a reliable and objective time reference suited to requirements

3.34
time-stamp token
data object that binds a representation of data to a particular time (expressed in UTC), thereby providing evidence that the data existed at that time

3.35
transferability
ability to recover an authentic digital archive (information, data, objects and all related metadata from one information system) in order to transfer it to another information system by means of a procedure specified in advance

NOTE This issue is of particular importance when information is stored by a third-party archive service provider.

3.36
trusted third-party archive service provider
third-party individual or organization in charge of archives preservation

4 General characteristics and levels of requirements

4.1 Characteristics

In order that an organization might apply a recognized specifications framework for the storage, use, archiving, retrieval and display of electronic documents, both technical and organizational measures need to be taken to ensure document integrity and long-term preservation.

In this context, an electronic information system shall implement a pre-defined archival policy; a description of the general principles of such a policy is described in Annex A.

It is important to recognize that information systems will capture electronic documents that are being submitted for long-term storage and use. The term “capture” in this sense reflects the receipt and processing of information to be managed by the information system. Where hardcopy documents need to be stored and managed in electronic form, these documents shall be scanned and indexed prior to their capture in the information system.

This part of ISO 14641 is applicable only to unalterable captured documents. Related document reference data in the file system or database shall not be erasable, changeable or able to be replaced by new data.

Procedures and security requirements shall be implemented in order to:

a) control the process of archiving;

b) prevent and/or detect modifications made to documents or to the data necessary for their retrieval and display;

c) ensure the integrity of audit trail data (including the log of the system events).

An electronic information system shall feature characteristics of:

1) suitability for long-term preservation;

2) integrity;

3) security;

4) traceability.

This part of ISO 14641 outlines:

— specifications for procedures relative to the processing, preservation, access and restitution of scanned or digitally born information, and requirements for the security of the information system;

— procedures relative to the digitization of analogue documents;

— procedures relative to the capture of documents, their preservation, access and restitution;

— procedures relative to the potential disposal of documents;

— rules relative to applicable procedures concerning operators;

— description of the resulting attestations of these operations;

— specifications concerning materials, equipment and software implementations;

— conditions of system audits and related procedures;

— characteristics applicable to the use of trusted third parties;

— characteristics applicable to the use of subcontractors.

The technical description manual, attestations produced and logs detailing the lifecycle of archives or system events shall be kept in the same conditions as the archives themselves.

4.2 Levels of requirements

Different organizations might have distinct and individual approaches to risks and requirements for information systems used for the preservation of electronic documents.

Table 1 outlines degrees of levels of these requirements. It summarizes general characteristics and practical methods for implementation at the level of requirement preferred by the organization, with regard to the nature of documents to be preserved and potential risks incurred.

Additional requirements may be selected based on specific needs and acceptable levels of risk.

The conformity of an information system with this part of ISO 14641 shall be evaluated in relation to the level of requirements selected by the organization.

Table 1 — Requirements of information systems

Characteristic	Minimal requirements	Additional requirements
Suitability for long-term preservation	Use of standardized or industry-standard and publicly available file formats	Format conversion Document scanning
	Metadata description of document	Standard metadata format
	Migration of media	
	Format conversion	Control and conversion of formats at time of capture Format obsolescence alert Planned and traceable format conversion
	System change management	
Integrity	Guaranteed by storage on media: — physical WORM — logical WORM on fixed media with — events log — techniques and procedures for detection and prevention of substitutions of input — logical WORM on removable media (see rewritable/erasable media) — rewritable/erasable media (normal security level)	 Strong security level Advanced security level Strong security level Advanced security level
	Capture process of archives	
	Alerts prior to destruction of archives	
	Description of the process of destruction of archives	Definition of change procedures for preservation periods Post-destruction preservation of metadata and audit trail

Table 1 *(continued)*

Characteristic	Minimal requirements	Additional requirements
Security	Identification of persons and processes accessing archives	Strong authentication
	Backup copies of archives	Use of different types and forms of media Protection from risks of flood, fire, etc.
	Controlled archiving operations (identification and traceability)	Strong authentication Retrieval in formats other than input formats
	Continuity of access to archives	
Traceability	Date and time stamp	Date and time stamp from trusted third party
	Maintenance of a technical file (archival policy, general conditions of services, operations procedures, lifecycle of document)	Adjustment to the organizational processes of the customer and related attestations
	Maintenance of an audit trail of archives lifecycle and events log	Digital signature and date and time stamp of attestations of operations and events, in units or batches Definition of the granularity of the batches of events to which a digital signature applies Frequency of archiving of audit trails and logs

5 General specifications

5.1 General

The design and operation of the information system shall allow implementation of procedures guaranteeing the requirements selected from 4.2.

5.2 Technical description manual

A technical description manual of the information system shall be created and retained. It shall contain at least:

a) a list of hardware components of the information system with all serial numbers affixed by manufacturers, the key features of these components, date(s) of production, compliance with related safety standards;

b) for a network system, its typology and topography, as well as a description of the connections and security equipment;

c) a data architecture model of information objects and their relationships, with regard to their use in support of the general objectives of the information system;

d) a list of software products and related documentation, identification of installed versions and dates of installation of these versions;

e) a list of customized software applications with their design/architecture file, their source code or proof of their deposit in custody;

f) a description of the interactions between the diverse components of the information system;

g) a description of the physical environment (temperatures, minimum and maximum humidity, etc.) in relation to specifications provided by the equipment manufacturers for proper functionality and preservation of information media;

h) a description of the technical and physical environment for the satisfactory functioning of the information systems (e.g. type of power supply, generator, system of fire detection, redundancy implementation);

i) a description of the physical protection measures for safety and security (guarding, remote detection, safes, locks, electromagnetic protection, etc.);

j) a description of the maintenance requirements for the information system.

5.3 Archival system profiles

An archival system profile is a set of rules applicable to documents sharing the same criteria of confidentiality, duration of preservation, destruction and access rights for capture, retrieval or disposal. These rules also specify the metadata which need to be associated with documents managed in the profile.

An archival system profile shall specify in particular the rights of persons and/or applications authorized to:

a) modify an archival system profile;

b) make a deposit;

c) access (view or play) a deposit;

d) prolong or decrease the duration of a deposit;

e) delete or dispose of a deposit, either prematurely or as planned.

Any creation, modification or deletion of an archival system profile shall be archived in an archives lifecycle log held under the responsibility of the archiving service of the organization, or by a trusted third party.

An archival system profile can be defined for individual electronic documents. However, for bulk archiving, this could be extremely time-consuming. Consequently, in this case it is preferable to use a set of predefined rules grouped together in a more general archival system profile.

5.4 Operational procedures

5.4.1 General

The organization shall set up procedures for the capture, storage, access and restitution of documents. These procedures shall be detailed in the technical description manual and shall include at least the following information:

— techniques and procedures used for search and printing;

— techniques and procedures for production of all types of attestation;

— techniques and procedures for storage and preservation of media and of storage infrastructures;

— file formats used;

— techniques and procedures for duplication and replication of documents and backups;

— techniques and procedures used for digital encryption and data integrity.

5.4.2 Scanned documents

In addition to the procedures defined in 5.4.1, where document scanning is undertaken, the following procedures shall be included in the technical description manual:

— techniques and procedures used for digitization (a description of the document to be scanned and of any particular distinctive features, preliminary operations needed, such as selection of output formats, imaging resolution, compression technique, if used, reconditioning of the document after digitization, if applicable, etc.);

— techniques and procedures used for indexing (location of the document, identification references on the document, on equipment or on accompanying vouchers, identification references of electronic messages);

— techniques and procedures for related metadata and any related enrichment of related metadata;

— techniques and procedures used for quality control (use of test targets for digitization, page count of scanned batches, electronic messages filter control, code controls, if any, with regard to reference tables, etc.);

— techniques and procedures used for the destruction of the source document, if applicable.

5.4.3 Digitally born documents

In addition to the procedures defined in 5.4.1, where digitally born documents are involved, the following procedures shall be included in the technical description manual:

— techniques or procedures used for transfer, receipt and control of documents to be archived;

— techniques and procedures for related metadata and any possible enrichment of related metadata;

— techniques and procedures concerning conversion of digital document formats during capture to the information system, or later if formats become obsolete.

5.5 Security

5.5.1 Management and organization of security

All organizations shall have a management procedure in place to ensure the security of their information system.

NOTE For security requirements, reference should be made to ISO/IEC 27001 and associated standards.

The management system for security shall be distinct and separate from the administration of information system operations or telecommunications systems. Its structure and governance shall be clearly defined and communicated to all personnel of the organization.

The administration and organization of security of the information system shall apply principles inherited from a general strategy or policy of the organization and rules already in place, notably:

— management of the keys of premises;

— security systems for detection, intrusion and alarms;

— compliance of hardware with regulations concerning human safety (see IEC 61000-4);

— operation of software products, the sources of which are known and available;

— development of adequately documented and tested custom software;

— management of access profiles to the information system (directory);

— use of transmission networks with features for integrity checks, safety and security operators;

— employment of third-party providers (security, guarding, cleaning, maintenance).

5.5.2 Risk assessment

Security measures are often developed using an ad hoc approach, in reaction to security incidents or the availability of computer software tools. Such procedures frequently leave gaps in security, which are only filled at some later date. A more structured approach is to review the information assets of the organization, and assign risk factors (based on asset value, system vulnerability and likelihood of attack). An information security policy can then be produced and approved, against which security measures can be audited.

The organization shall undertake an information security risk analysis, and document the results obtained.

Of particular importance are the security measures implemented to control the information storage media, both the live media and the backup media. The risk analysis shall include vulnerability risk factors consistent with the type of media being used (e.g. WORM or rewritable).

Where different types of storage media are used, their impact on the risk analysis results shall be reviewed.

Once the risk analysis has been completed, it shall be acted upon as part of a review of implemented security measures. Factors such as the balance between the costs of implementation, security achieved and risk evaluation shall be taken into consideration during the review process.

Based on the results of the risk analysis, existing security measures shall be reviewed for effectiveness.

Where the review indicates that changes to security procedures are appropriate, the identified changes shall be implemented.

5.5.3 Physical security

Measures shall be taken for physical security, including the prevention of unauthorized access to hardware, to telecommunication systems, to media holding information and to information ensuring their retrieval and display, audit trails, logs and backups.

If continuity of access is needed, it is advisable to use several secure premises to minimize risk, using different sites for media and/or systems containing backups (copies) of information and mechanisms for their operation.

Removable media shall be continuously monitored during their handling and/or transfer from one protected location to another. It shall be possible to identify all holders of all media at any point in time.

When removable media are not actually in use, it shall be stored in specific protected locations.

If the destruction of physical documents is envisaged, specific procedures for the security of these operations shall be implemented, both for original analogue paper-based documents and for digitally born documents.

If media containing documents need to be disposed of, appropriate measures shall be taken to make it impossible for reconstruction of information initially held on the media.

5.5.4 Hardware security

Security measures covering hardware and software contribute, either separately or jointly, to the security of information systems by allowing for:

a) identification of hardware configurations, including peripherals;

b) controls guaranteeing the absence of malicious or accidental modifications of hardware configurations;

c) controls guaranteeing that only authorized users can access the hardware.

Accordingly, security issues shall be taken into account when choosing equipment and during their installation and implementation.

To limit the risks of illegal interceptions of information by third parties due to the transmissions of involuntary electromagnetic radiations, it is advisable to test the hardware for compliance with IEC 61000-4.

5.5.5 Security of custom software and software products

Custom software and software products are integral to system configuration; accordingly, they shall be subjected to the same safety conditions as the hardware.

The operating systems and software products that are chosen shall provide:

— access control tools for enhanced protection;

— protection against intrusion and malicious software;

— controls ensuring the absence of accidental or malicious changes to software configurations.

The security of software shall be ensured using:

— access controls guaranteeing that only authorized users can use the software and the information which they are entitled to access;

— detection and monitoring systems so that any unauthorized access attempts are discovered and reported.

It is advisable to use software which is in the public domain or, where possible, to obtain sources from the supplier.

Rigorous methods shall be used for the development of software; the selection of best practices and checks shall be the responsibility of the person in charge of the application.

Before being put into service, software and software products shall have been adequately tested on a machine other than the main production machine, or on a production machine during periods of operational down-time, having previously backed up data and indexes and having removed all appropriate removable information system media.

Security of access and granting of access rights to the information system shall be carefully studied, designed and implemented from the beginning of the system design.

The software and software products shall be specially protected, and access rights enabling their change or modification should be granted only to authorized persons.

In cases of malfunction, a report shall be immediately delivered to the security authority and the malfunctioning part of the information system shall be isolated as quickly as possible.

5.5.6 Maintenance of the information system

Information describing every maintenance operation shall be recorded in the technical documentation of the information system. This shall include an identification of the maintenance operation, either preventive or curative, entrusted either to the organization, or to specialized third-party providers.

Removable media containing electronic documents and their related metadata shall never be left in drives during maintenance operations.

If media are not removable, a valid backup copy shall be created before any maintenance operation (see 5.5.8).

All tests shall be made with removable media specifically allocated for this task. If media are not removable, it shall not be possible for tests to alter or destroy recorded information.

Preventive maintenance shall be performed to ensure proper functioning of the information system. In particular, regular checks of removable disk drives or fixed media shall be made to verify that these are in proper working order according to manufacturer recommendations.

5.5.7 System change-management and migration of media

Periodic upgrade operations and modification or replacement of hardware or software shall be planned in advance of their implementation.

All these operations shall be detailed in the technical description manual of the information system and registered in logs.

The long-term preservation and integrity of the documents and their metadata shall be ensured when implementing periodic upgrade operations.

The following two situations may apply.

a) The new storage media are capable of being read by the former information system; all media shall be checked for legibility on the new storage media hardware before retiring the former storage media.

b) The new storage media cannot read media used by the former information system; all documents contained on former media shall be copied to the new media on a hardware system which temporarily uses both types of storage media.

5.5.8 Security backups

The information system implementation shall keep at least two copies of the same information at all times, preserved in two geographically remote locations. At least one copy shall be written to non-alterable media.

The media used for security backups may be of a different kind and type to the primary media.

When the media are of a non-removable type, two information systems in geographically remote locations shall be implemented.

When the media are of a removable type, recording documents on backup media shall be performed as promptly as possible to allow for storage in a separate location to the primary location.

Each time a security backup is made, details of the process and the names and characteristics of backup files shall be recorded in the events log.

5.5.9 Continuity of access to archives

As with any information system, a disaster recovery procedure (also known as a business continuity plan) shall be available and documented.

This procedure shall permit system restoration without any loss of data, metadata, logs or any other sets of data (users list, archival system profiles, etc.).

The software and procedures to restore system data shall be described in the technical description manual.

The implementation of the information system shall ensure that the last validated document cannot be lost at any point in time.

The information system shall automatically create a record of any restoration processes.

5.6 Date and time stamping

In the framework of this part of ISO 14641, there are two possible types of date and time stamp, depending on the mode of delivery (internal or trusted third party), which shall include at least the following characteristics:

a) creation of a time stamp in accordance with applicable standards;

b) preservation of a date and time stamp token for required periods;

c) source of reference time;

d) verifiable operations policy for date and time stamp.

For related operations the selected form of date and time stamp shall be described in the technical description manual.

The formats of dates and times shall be compliant with ISO 8601.

The date and time stamp shall produce a complete date with hours, minutes, seconds and fractions of seconds displayed according to the following format:

YYYY-MM-DDThh:mm:ss.sTZD

where

YYYY indicates the year using 4 characters;

MM indicates the month using 2 characters (e.g. 01=January);

DD indicates the day using 2 characters (01 to 31);

hh indicates the hour using 2 characters (00 to 24);

mm indicates the minutes using 2 characters (00 to 59);

ss indicate the seconds using 2 characters (00 to 59);

s is one or several characters representing a decimal fraction of a second;

TZD indicates the time zone (Z for UTC or +hh:mm or -hh:mm).

EXAMPLE 2007-08-29T09:36:30.45+02:00

It is important to select the degree of precision of the measure of time in order to determine what the highest rate of occurrence of events in the information system is and then to select a unit of time small enough to ensure that two events of this type will not carry the same date and time.

For date information, Coordinated Universal Time (UTC) shall be used.

The technical description manual shall specify time sources and update methods and controls, as well as the synchronization processes of the various clocks of the information system.

If a date and time stamp token is required for an information system, it shall be provided by an attestation creation unit (ACU) or by an independent trusted third party external to the information system.

5.7 Audit trail

5.7.1 General

Any event associated with the information system or with the lifecycle of documents shall be recorded. Event logs shall be automatically produced by the information system with a date and time stamp (see 5.6). A full description of the events shall be recorded sequentially in the relevant logs.

All logs shall be described in the technical description manual, with all related administration information. Logs shall be easily accessible and legible.

Logs shall be archived on a regular basis according to the same archival policy as related documents, on storage media providing the same characteristics of preservation and integrity.

Event logs shall not be accessible to regular users and operators; administration of logs shall be restricted to a duly designated operator.

The production of event logs entails the production of electronic attestations. These shall be archived in the same conditions as related documents.

5.7.2 Secure preservation of the audit trail

Whatever type of media are used for audit trail preservation, the audit trail shall demonstrate proof-of-continuity of capture of events of the information system.

Logs shall be stored and kept in the same secure conditions as documents.

5.7.3 Archive lifecycle log

A log of the lifecycle of archives can be general or specific to each entity.

It shall include electronic attestations, namely:

1) attestation of initial deposit;
2) attestation of modification of the duration (retention schedule) of a deposit, if any;
3) attestation of deletion, either premature or at term of a deposit, if applicable;
4) attestation of restitution of a deposit, if applicable;
5) attestation of any creation, modification or deletion of an archival system profile.

The log of the lifecycle of archives shall be updated at the time when the log of creation, modification or deletion of an archival system profile is generated, or when a new electronic attestation is issued.

Any user accredited in an archival system profile as an authorized operator shall be able to view, partially or completely, the log of the lifecycle of archives.

The archive department of an organization, or a third party, shall provide user accreditation in an archival system profile as an operator, including all means necessary to control the integrity and provenance of all or part of the log.

After each update, or at any time, the archive department of an organization, or of a third party, shall allow accredited persons to check the integrity of all or part of the log.

5.7.4 Events log

The events log shall be unique to an information system and shall record who used it (whether a human user or an automated-system user), when it was used, what was done to the information system and the outcomes. The events log shall track who has accessed the information system, whether the personnel have respected the procedures, or whether any action taken could have been accidental, fraudulent, malevolent or unauthorized.

The events log shall contain three sections:

a) a section for all events related to the archive application;

b) a section for all events related to security;

c) a section for all events related to the information system.

The main function of the events log is for internal verification. It shall allow review of all information, error messages and other alerts generated during information system operation, such as task failures or execution.

For information systems using physical or logical WORM media, the events log shall record start-up and shut-down of each medium. In the event that one medium is copied to another, the events log shall record this action.

The information in the events log shall provide evidence showing that specified procedures have been followed and shall include at least the following information for each significant event:

— date and time of the operation, in accordance with ISO 8601;

— operation performed;

— identification of the technical components used;

— title of the process involved and its version;

— identification of the operator, if applicable.

6 Storage media considerations

6.1 Media type definition

Table 2 gives definitions of different media types.

Table 2 — Definitions of media types

Type of media	Definition
Removable media	Physical media recording information which can be removed from the drive. Technologies can be optical or magnetic, on disk or tape.
Non-removable media	Physical media recording information which are an integral part of the drive, and which cannot be removed from it. Technology is mostly magnetic on disk.
Physical WORM	The information is written once using a physical non-reversible once-only modification of the media. After this modification it is not possible to modify or delete the information.
Logical WORM	The media use rewritable technology, but hardware or software devices prevent any modification or deletion of any recorded information.
Rewritable	On these media, information can be recorded, modified or deleted without any restrictions.

Table 3 shows the clauses of this part of ISO 14641 that describe the uses of different media types in an information system complying with this part of ISO 14641.

Table 3 — Uses of different media types

Media disposition	Media type		
	Physical WORM	Logical WORM	Rewritable
Removable	Clause 7	Clauses 7 and 8	Clauses 7 and 9
Non-removable	—	Clause 8	Clause 9

6.2 Preservation of archival media

Archival media, whether removable or non-removable, shall be kept in an environment compatible with their physical properties, as described by the manufacturer or according to relevant applicable standards.

The state of recorded data shall be controlled regularly. A quality process shall be associated with controls and the periodic examination of media. This process is a key factor for ensuring the preservation of recorded data on media.

Transfer of recorded data to new media shall be done according to the media's life expectancy, as recommended by the manufacturer, or when a test of the media produces results showing that the media characteristics are close to their recommended value limits.

Change of media shall guarantee the long-term preservation of the integrity and access of documents.

7 Systems using removable media

7.1 General

Storage media are not usually directly addressed by an information system. Information is actually recorded on storage volumes.

A storage volume can include one or more storage media, and media storage can be part of one or more storage volumes. Media storage is a physical reality, while storage volume is a logical virtual notion.

When removable optical media are used, volume and file structures shall adhere to either ISO/IEC 13490 or ISO/IEC 13346.

7.2 Initialization of removable storage volumes

A history of the hardware configurations used when recording documents shall be retained, as technologies are in constant evolution.

Storage volumes shall be mounted, prior to the recording of the first document, with the following information:

a) unique identification of the media;

b) mount date and time;

c) name of the organization.

7.3 Finalization of removable storage volumes

When a volume is full, and after the last document has been recorded, it shall be finalized, where possible. Accordingly, the following information shall be registered after the last user information:

a) the date and time of finalization;

b) the number of files stored on the media.

Finalizing a volume shall prevent any further writing to this volume.

7.4 Labelling of physical WORM media

When using physical WORM media, information system security depends on the identification of media and the existence of an events log recording any migration of these media.

As a result, it is necessary to be able to identify each physical WORM medium individually and to specify techniques and procedures enabling detection and/or prevention of any substitution of media. The technical description manual shall describe the way this is done.

8 Systems using logical WORM media

As logical WORM media are by definition physically rewritable, information systems using both non-removable and removable logical WORM shall be considered, in the context of this part of ISO 14641, as information systems using rewritable media.

In addition, when using removable logical WORM, the requirements in Clause 7 shall apply.

9 Systems using rewritable media

9.1 General

When an information system uses removable or non-removable rewritable media, preservation of integrity relies on the rule that once an entry has been made it cannot be modified without this being detected and registered using cryptographic techniques and the production of electronic attestations.

Three levels of security can be referenced: standard, strong and advanced. These levels require the use of distinct cryptographic techniques: hashing functions, date and time stamps and/or digital signatures.

When a security level entails the use of a digital signature, the signatory directs and activates the tool creating the digital signature. The signatory can be an individual, an organization or a process. Where the signatory is a process, the digital signature shall be automatically produced at the time of the occurrence of the related operation.

The advanced digital signature shall adhere to the following requirements:

a) it is uniquely linked to the signatory;

b) it is capable of identifying the signatory;

c) it is created using means that the signatory can maintain under his sole control; and

d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

NOTE An advanced digital signature corresponds to the definition given by ETSI (European Telecommunications Standardization Institute) in the following specifications: ETSI TS 101 733 (CAdES) or ETSI TS 101 903 (XAdES).

For each of these three levels of security, an electronic attestation shall be issued and registered in the audit trail, confirming initial deposit of documents. It shall include at least the digital fingerprints of archived documents and a logical storage address, independent of storage location. Attestations shall provide evidence that related operations have been requested by an authorized person and performed under the full control of the information system of the organization or third party.

9.2 Standard security level

At this level any person or process authorized by an archival system profile to perform an operation shall at least be authenticated using an identifier and password, conforming to the security policy of the organization or the third party.

In order to prevent any modification of an entry in the lifecycle log of the archives, the log shall be date and time stamped at least once a day, even if there was no activity during this day. The continuity of the log shall be preserved.

This security level shall be supported by audit trails managed by the information system of an organization or a third party.

9.3 Strong security level

At this level the following conditions are additional to those of the standard level.

Each attestation entered in the information system log shall be signed electronically by the ACU of the information system of the organization or third party.

The information system of the organization or the third party shall state, for each archival policy, the signature policy or policies defined for attestations electronically signed by the ACU.

9.4 Advanced security level

At this level the following conditions are additional to those of the strong level.

Any persons authorized to do so by the archival system profile shall sign requests using an advanced digital signature. Each attestation shall include the signed request, which includes a countersignature as specified in the strong security level.

The archival service of the organization or the third party shall specify for each archival policy the signature policy or policies applying to requests electronically signed by persons authorized by the archival system profile to perform operations.

10 Archival capture

10.1 Electronically born documents

10.1.1 General

Electronically born documents received by the information system shall be preserved using a standardized or industry-standard file format. Specifications of formats shall be freely available for the complete lifetime of the document. In the archival policy, the referenced standard associated with each distinct type of related document shall be noted. This also applies to format specifications, in order to ensure long-term usage and information content fidelity.

10.1.2 Procedure for archives capture (deposit)

Two distinct and linked operations are mandatory for capturing archives: capturing archive files to archival media and updating catalogues with the associated metadata. Capture is only valid if both operations are achieved.

Processes for the control and capture of documents and their associated metadata shall be specified.

Electronic documents shall be captured to the storage media using unique file identifiers.

For each archival deposit, the information system shall at least:

a) check that the quality of the document recorded on the archival media is correct, using any error detection and correction codes that might be available on the devices used;

b) validate that the new document has been registered in the information system catalogue;

c) secure the link between the physical location of the document and its logical identification.

10.1.3 Marked-up electronic documents

This includes documents made of textual and/or non-textual components, structured by XML standardized markup. This type of document can refer to a logical model, referenced at the beginning of the document.

Archiving of this type of document shall include all constitutive components, i.e. technical description diagrams, codification tables, linked documents, etc.

10.1.4 Electronic documents using a layout format

This signifies an encoding format for viewing and printing a document. Formats used for archival purposes shall be standardized or industry-standard, with published specifications freely available for the complete lifetime of the document.

NOTE Formats described in ISO 19005 (all parts) conform to this requirement.

10.1.5 Other electronic document formats

If the decision is made to keep an electronic document in its native format, and when this format's specification is not publicly available, the preservation of the document in its native format might call for the preservation of related hardware and/or software tools for access to the information.

10.1.6 Print streams

This subclause deals with files sent to high-volume printers. Together with data to be printed, such files may contain references to external files called “resources”. Such “resources” may comprise fonts, images, overlays, forms, etc. These “resources” are necessary for display and rendition of the electronic document.

The files representing the document and all associated resources needed for rendition shall be stored under the same conditions in order to preserve the links between all components.

For this type of electronic document, all referenced files shall use a standardized or industry-standard format. The set of files making up the electronic document shall allow the restitution of the original printed document without transformation.

10.1.7 Verification of electronic documents

Checks shall be made for at least:

a) quantity and volume of deposited documents;

b) compliance of associated metadata with specified formats;

c) either absence of coded data or, alternatively, legible values, permitting interpretation of codes.

Supplementary checks that can verify compliance of deposited documents with formats specified in the archival policy shall be made.

10.1.8 Integrity control of electronic documents transferred from source applications

The integrity of documents, or batches of documents, received from external production applications shall be verified before their uploading in the information system.

Two cases have to be considered:

— if the documents or batch of documents already contain a digital seal, the seal shall be checked when receiving the transfer into the information system;

— if the documents or batch of documents do not contain any device allowing such control, then the integration of an appropriate means shall be considered.

10.1.9 Metadata capture

Metadata can be obtained in several mutually compatible ways:

a) automatic extraction of metadata from the document;

b) automatic extraction of metadata from the information system which created the electronic document;

c) metadata input or enrichment during capture.

Procedures to create and control metadata shall be described in the technical description manual.

When capturing electronic documents, metadata shall include the following information about the creation or origin of these documents:

— identification of the entity originating the transfer of the documents;

— identification of the archival service receiving the documents;

— the date and time of creation or arrival of the transferred archival batch;

— the conversion technique applied to the original documents if the native format of the documents does not conform to 10.1.1;

— the encoding format of the documents;

— the preservation period (retention schedule) and final disposition of the documents;

— access rights associated with the documents;

— the size of the archival batch.

10.1.10 Indexing and document searches

Electronic documents shall be classified, identified and indexed using a method that enables the search for a particular document or a particular set of documents.

These indexes shall be constructed from the metadata of the documents. Indexing information shall be preserved by the information system either as a simple and autonomous index, referring only to the documents, or as part of a more complex information system (e.g. as part of a larger database).

The information system shall be designed in such a way that inadvertent user actions do not, without due warning, result in modification or loss of the indexes or of the links between the logical address and the physical address of the documents.

10.2 Paper-based or microform documents

10.2.1 Scanning devices for documents

Scanning devices for documents initially on paper or microform shall be fully described, including:

a) physical characteristics of documents handled by the scanners;

b) capture capacities of the scanners;

c) optical devices of the scanners, if applicable, with their operational and available tuning mechanisms;

d) tuning mechanisms of the scanners and their related operation.

10.2.2 Image processing features

To produce quality digital images or to reduce the size of files, it might be necessary to use software or hardware devices that enable processing of these images after digitization. The effects of each process and their limitations shall be specified in the technical description manual.

The most frequent techniques are:

a) image transformation from colour or grey scale to monochrome;

b) deskew;

c) despeckle/background cleanup;

d) black-border removal;

e) removal of overlays, logos, watermarks or any other type of unrelated information;

f) removal of blank pages.

All these processes shall be implemented with careful consideration as they have a bearing on the fidelity of the electronic image in relation to the source document. In particular, the procedure for converting a grey-scale or colour image to a monochrome image shall have been tested and validated in detail prior to its implementation.

Speckle removal can lead to the deletion from an image of certain items of information, such as a comma or an accent or a detail in a diagram. It shall therefore be tested before implementation. The test results shall be stored in the technical description manual.

The software used for removal of overlays, leaving only the variable content, can be used if the related features operating in the information system are fully specified in the technical description manual. In addition, when the retrieval of a document requires merging the variable content and the overlay, then the version of the overlay used shall be identical to the overlay extracted when the page was scanned and processed.

The technical description manual shall describe the management of overlay versions and the logical link between a document's variable content and the corresponding version of the overlay.

Overlays are considered as elements of the document and shall therefore be stored in the same conditions as other document elements.

When it is mandatory to preserve the information as a whole, it is advisable not to use such techniques. In all other cases, it is necessary to specify the reasons for the use of such techniques in the technical description manual.

Blank page removal could represent a potential risk of information loss. When this is implemented it is advisable to check that the technique used is reliable and does not delete pages containing information. The technical description manual shall specify the procedures used to ensure the reliability of this operation. It is also advisable to implement a process which will count the number of removed pages relative to the number of retained pages.

The use of test targets (see ISO 12653-1 and ISO 12653-2) allows objective measurement of the information system and to check the effects of image processing software.

10.2.3 Paper document or microform capture procedure

10.2.3.1 General

When paper-born or microform document capture has been completed, the operator shall deliver a scan attestation that at least provides the operator name, scan date, time of scan start and finish, identifiers of the first and last document scanned and the number of pages scanned.

After checking scanned images, an authorization attestation shall be issued by the owner or the authorized agent of the owner. If the attestation applies to a batch of documents, the number of images and documents shall be specified.

10.2.3.2 Preparation of paper documents

The organization shall ensure that the quality of paper documents it produces is compatible with the scanning or micrographic capture techniques. Torn or creased documents, whether issued by the organization or received from external sources, can require reconditioning before digitization. Nonetheless, the text of the documents shall neither be modified nor corrected in order to improve legibility, as this could alter the integrity of the documents in relation to the original documents.

Whenever possible, measures such as those stipulated in ISO 10196 and ISO 12029 shall be implemented for the processing of documents intended for digitization.

10.2.3.3 Preparation of microform documents

Microform documents shall, if necessary, be cleared of dust before digitization. The operator shall check if there are any scratches or defects limiting legibility to the point where document reading or processing will be rendered impossible.

10.2.3.4 Paper or microform document scanning

The user manual shall specify all details relating to document scanning, scanner tuning, image enhancement processes and the different elements of the scanning procedure. Any processing technique used to enhance information shall be approved beforehand with the project originator and fully described in the scanning system user manual.

The user manual shall cover all topics related to the authorized operations concerning digital image modifications produced by document scanners.

10.2.3.5 Verification of scanned information

The scanning system user manual shall include a procedure covering verification of scanning.

Verification checks shall at least apply to:

a) quality and integrity of images in relation to the source documents;

b) accuracy of the indexing information of the scanned documents.

If quality checks can be performed by operators themselves in order to reduce rejections, it is advisable that the final quality check be performed by persons other than the operators.

Sampling procedures for individual physical elements shall comply with ISO 2859 (all parts).

10.2.4 Audit trails

10.2.4.1 Document or batch identification

Document scans (paper or microform) shall include the following information history elements:

a) unique identifier of the documents in the information system;

b) number of pages of the documents.

Scan batches (paper-born or microform) shall include the following information history elements:

— batch identifier (this identifier shall be unique to each batch);

— number of documents/reels of microfilm/microfiche in this batch;

— number of scanned pages or, for microforms, the number of frames.

10.2.4.2 Document capture process details

The following information, if applicable, shall be recorded in the audit trail:

a) messages received from the scanning device (scan start date and time, batch initialization for automated systems, end of scan process, etc.);

b) quantity of bytes produced by the document scan process before and (if compression is used) after compression.

10.2.4.3 Audit trail data

A historical record of events shall include at least the following information.

For paper-born document digitization:

a) identifier of the first document or first batch of documents scanned and stored;

b) identifier of the last document or batch of documents scanned and stored;

c) date and time of arrival and departure of each operator;

d) identifier of the first document or batch of documents scanned and stored by each operator;

e) identifier of the last document or batch of documents scanned and stored by each operator;

f) total number of processed pages;

g) total number of pages not processed, including those impossible to scan due to the poor quality of the document (e.g. weak contrast, tears or shreds);

h) total number of blank pages, if any.

For microform digitization:

— identifier of the first microform scanned and stored;

— identifier of the last microform scanned and stored;

— date and time of arrival and departure of each operator;

— identifier of the first microform scanned and stored by each operator;

— identifier of the last microform scanned and stored by each operator;

— total number of processed microform frames;

— total number of non-processed frames, including those impossible to scan due to the poor quality of the microforms.

10.3 Analogue audio/video objects on tape media

10.3.1 General

This subclause relates to information systems that have devices for encoding (digitization) original audio and audiovisual recordings.

10.3.2 Preparation of original tape media

Before encoding (digitizing) magnetic tapes, these tapes shall be checked to evaluate the operational conditions of the medium and its recordings.

This check includes:

— the physical state of repair of the tapes,

— read performances, and

— the organization and quality of recorded sequences.

10.3.3 Original audio and audiovisual object digitization

The quality of the digital version of objects will be determined by the features of original object reader equipment and the digitization process (properties of converters and sampling/encoding methods). In some cases, procedures for cleaning and maintenance of the material shall be conducted before reading procedures. Reading devices shall be fine tuned (e.g. alignment of tape recorder reader heads, video recorder tracking).

The tools for the extraction of information, digitization and transfer conditions shall be fully described, including:

a) physical specifications of supported media for the digitization devices;

b) specifications and settings features of the reading devices (audio tracks, composite or component analogue video format);

c) specifications of the digitization devices.

10.3.4 Audio and audiovisual information processing

When the preservation of information integrity is mandatory, any kind of processing that could result in a modification of the information in relation to the original shall be excluded or limited as far as possible.

When information modification is possible, in order to enhance acoustic or visual quality, processing software may be used, providing that each function has been tested and validated before use. The functions used by the information system shall be fully specified in the technical description manual.

10.3.4.1 Audio objects

For these types of objects, usual tunings are:

a) tape-speed tuning;

b) spectral balance adjustment;

c) acoustic level adjustment (set or dynamic compression);

d) removal of temporary defects;

e) broadband noise reduction;

f) CODEC (compression/decompression feature) selection for encoded digital objects;

g) sampling frequency treatment.

Any “blank” removal actions shall be carefully considered and validated.

10.3.4.2 Video objects

For these types of objects, usual tunings are:

a) black-level setting;

b) luminance and colour increase;

c) video signal increase;

d) temporary defect reduction;

e) de-interlacing.

All these processes shall be implemented with careful consideration as they will have an impact on the fidelity of the digital sound or video sequence in relation to the original.

10.3.5 Events log

10.3.5.1 Object identification

For each object, the following information shall be recorded:

a) unique identifier of the physical object in the information system;

b) identification of entries.

10.3.5.2 Object batches identification

Logs for scan batches of objects (paper or microform) shall contain the following information:

a) batch identifier (this identifier shall be unique);

b) number of objects, reels or cartridges in each batch;

c) number of tapes and entries digitized.

10.3.5.3 Object capture and storage procedures verification

When these procedures are implemented, the following information shall be recorded in the log:

a) devices used for the operations (reading mechanism, converter, etc.) on selected formats and settings;

b) names of digital objects, lengths of associated sequence units;

c) quantity of bytes produced by the digitization of objects or batches of objects before and after sequence compression (if any).

10.3.5.4 Operations log

An operations log shall provide a historical trace of all operations performed daily. This log shall include at least the following information for the digitization of analogue audio/video objects from tape:

— identifier of the first object or first batch of objects digitized and stored;

— identifier of the last object or batch of objects digitized and stored;

— date and time of arrival and departure of each operator;

— identifier of the first object or batch of objects digitized and stored by each operator;

— identifier of the last object or batch of objects digitized and stored by each operator;

— total number of tapes or cartridges or items processed;

— total number of tapes or sequences not processed, including when digitizing was impossible due to the poor quality of the object (e.g. track alignment, breaks or stretching, friction);

— total number of blank tapes and length of blank sequences, if any.

10.4 Image, audio and video information compression techniques

10.4.1 Compression types

Files which contain digitized images of an analogue-born object can be compressed to reduce the disk space required for storage.

There are two different compression methods: “lossless” or “lossy”.

A lossless compression is performed when, after decompression, the image produced is exactly the same as the original object, bit by bit.

A lossy compression is performed when, after decompression, the image produced is not exactly the same as the original. In this case, part of the information of the original object is lost.

10.4.2 Paper or microform documents

Lossy compression shall be used only for colour or greyscale photographic type images when the compression does not lead, after a compression/decompression cycle, to a visible removal of information.

Lossy compression shall not be used for black-and-white documents, often referred to as office documents, which mainly contain text and/or line drawings. For this kind of document, a test target shall be used (see ISO 12653-1 and ISO 12653-2).

Some compression techniques allow a quality parameter setup. This parameter shall be set so that there is no apparent loss of information between the original image and the image which has undergone the compression/storage/decompression cycle.

Information systems shall provide means of verification after compression of files which contain images.

The compression type and, if appropriate, the parameters used for compression, shall be stored as an integral part of the file containing the digital image.

Any selection of a compression technique for the archival solution shall refer to ISO/TR 12033.

Whatever choice is made, the compression techniques shall be standards based and their specifications openly accessible. The technical documentation shall refer to the associated standard.

10.4.3 Audio or audiovisual recordings objects

Generally, audio objects shall not be processed using a lossy compression technique.

For video objects, considering the storage volumes involved and the bandwidth available for transmission, it is usually necessary to implement lossy compression.

For both audio and audiovisual objects, only ISO/MPEG-standardized formats shall be used. These standards offer choices for compression techniques and format which shall be selected for rendering information according to the quality requirement.

10.5 Format conversion

A table detailing the input formats accepted by the information system shall be created.

Encoding formats based on publicly available specifications (standards based, whenever possible) shall be selected. The selection of a conversion format shall be made according to the electronic document type and the characteristics that are to be preserved, or not, after conversion. It is important to determine whether the visual appearance (presentation) of the documents has to be preserved, whether there are any links to external documents and whether mathematical formulae or internal document macros have to be retained.

Selection of a new format for preservation, and related conversion techniques, shall avoid the accidental removal of significant information. Conversion characteristics and implementation shall be checked and recorded in the events log with the following:

a) name of program(s) used for conversion;

b) name of program(s) which enabled identification and validation of the format;

c) event type;

d) conversion date;

e) input file name;

f) output file name;

g) display of the format;

h) outcome of the operation (i.e. success or failure) and, when failure occurs, record of resulting anomalies.

Format conversions may be done at a number of different stages of the archival process: when a document is captured, when the conversion has been planned after document archival, or when the encoding format of an archived document has become obsolete and could present a problem for access.

The scope of the processes relating to archived electronic document formats varies depending on contractual agreements between the archive originator and the archival service, and on the applicable archiving policy.

— At input into the information system, the following steps are taken:

  — format checks (or not) on archival start (based on the table of acceptable system-input formats);

- format conversions (or not) at input based on the results of checks or based on contractual conditions referring to the table of target archival formats.

— After input in the information system, the following steps are taken:

  - alerts to the owner (or not) if encoding format has become obsolete;
  - conversion (or not) by the information system when format obsolescence is reported.

The format check shall be made with a tool which allows for exact format identification, description and validation.

11 Archival operations

11.1 Scope

Operation of archives means the access, restitution and final disposal of archives.

11.2 Access

11.2.1 General

Access operations shall be based on search criteria and the subsequent transfer of electronic documents into their archival format.

In addition, access can include:

a) display of the documents on a screen;

b) print of a copy on paper or film;

c) playing of audio in appropriate acoustic conditions relative to the quality of the documents;

d) playing of video images in appropriate acoustic conditions relative to the quality of the document.

Methods used to retrieve and display documents shall be specified in the technical description manual.

Processing of document content shall not be allowed for the operation of retrieval and display, with the exception of decompression, format interpretation and ensuing technical processing, as well as any necessary adjustments to the physical or software characteristics of the retrieval and display devices.

If required, an attestation of conformity of the transferred copy shall be produced. This attestation shall include, in addition to the name of the person who issued the request and the name of the person who delivered the attestation, the metadata allowing for the identification of the document and providing an audit trail of the document lifecycle in the information system.

11.2.2 Digitized documents

Viewing and reading applications shall be independent from the tools that were used to create archived documents. Therefore, an electronic document should be captured in a software and hardware environment different to the environment used for viewing or reading.

If the digital conversion process for a paper-born or microform source document uses software that deletes overlays, or any other fixed elements, the principle of document fidelity in retrieval and display requires that the restored document aggregates fixed content with variable content. The information system shall guarantee that the versions of the overlay or fixed elements used are the same as those captured during digitization.

11.2.3 Marked-up electronic documents

When specific coding tables are used, they shall be available and accessible during access.

Access to these documents shall be performed using the relevant layout instructions.

11.2.4 Electronic documents using lay-out format

Access processes shall be limited to the assembly of different document components, according to the prescribed display rules and the intended display media, without any action on or processing of the content.

11.3 Restitution

Archives restitution, whether total or partial, means the transfer of archived documents to their originator or to a duly appointed third party.

Restitution shall be accompanied by the destruction (disposal) of the documents in the information system.

The restitution procedure and the technical details of transfer (restitution format and selected media) shall be specified in the technical description manual.

11.4 Archives disposal

The preservation period of archived documents (retention schedule) shall be managed in the information system either by use of a record of the preservation period in the metadata for each archived document, or by referencing each archived document in relation to a preservation-period table. The information system shall allow modification of the preservation period for a specific document.

Under the supervision of an authorized agent, and in accordance with the existing procedures, at the end of the preservation period the archives shall be deleted. This operation shall make removed documents definitively and totally inaccessible.

NOTE For additional information refer to ISO 15489-1, ISO 15489-2 or MoReq2 specifications.

When a removable storage medium is destroyed, the process shall ensure the total inaccessibility of information recorded on the medium.

Any retention of metadata and logs or audit trails related to deleted archives shall be specified in the contractual agreement or in the archival policy.

12 Information system assessment

12.1 General

12.1.1 Audits

The information system and all the related procedures shall be regularly audited, especially when major changes are made to the information system. These audits can be performed either by internal personnel of the organization responsible for the implementation of the information system (internal assessment) and/or by personnel provided by a third-party enterprise (external assessment).

The results of these audits shall be retained.

12.1.2 Objectives

Audits shall verify that the information system and procedures are compliant with this part of ISO 14641. This compliance control shall cover system design, implementation, use and all operational procedures.

Moreover, the audits shall be able to measure the efficiency of the implemented information system and its ability to address the objectives and requirements of the related field of activity.

Finally, audits shall provide all information useful for appropriate improvement of information system compliance.

12.1.3 Auditor responsibilities

Auditors shall at a minimum:

a) formulate and clarify the requirements;

b) prepare and carry out the audit operations with which they have been tasked;

c) record the results;

d) report the conclusions of the audits.

Auditors shall be impartial and free from any influences that could affect objectivity.

12.1.4 Personnel responsible for assessment

The qualifications, training and experience of each auditor (active or assisting) shall be controlled and monitored by the organization responsible for them.

More specifically, auditors shall be experienced, with several years of professional practice in the field of document management, electronic archival or records management. A significant proportion of this experience shall have been in the design of and consulting for the implementation of information systems.

Internal or external auditors shall have the following skills necessary to conduct the audit process:

a) techniques to measure, interrogate, assess and write reports;

b) techniques to run various audit processes such as planning, method, organization, communication and management.

Their skills shall be appropriate to cover all types of documents contained in the information system, including specific technical documents such as audio and video.

12.1.5 Verification of documentation

The organization shall maintain an information system which ensures that all documentation related to audits can be verified and which ensures that:

a) up-to-date versions of requisite documentation are available in appropriate quantities at all points where operations are made to the information system;

b) all changes or amendments to documentation are properly authorized and processed in such a way that ensures rapid and direct action of the personnel involved;

c) outdated documentation is promptly withdrawn and destroyed from all points of distribution and use in the organization (exceptionally, outdated documentation which needs to be preserved for legal or historical purposes shall be appropriately identified and preserved).

12.1.6 Assessment operations documents

The organization shall record all results of assessment operations. Documents shall describe the processes applying to each assessment operation.

All documents shall be securely preserved for an appropriate period.

12.2 Internal assessment

When an assessment is made by personnel under an organization's authority, the organization shall produce and be able to provide a description of the organization, clearly showing the distribution of responsibilities and hierarchical structure of the organization, in particular demonstrating the independence of auditing roles and operational roles.

12.3 External assessment

Third-party organizations providing information system audits shall have sufficient and adequate experience and skills in the design and implementation of information systems for document preservation.

Personnel carrying out assessment operations shall have appropriate qualifications, training and experience for the proper auditing of information systems.

Third-party organizations shall take all necessary measures at all levels of their organization to ensure the confidentiality of information collected during auditing.

13 Trusted third-party archival

13.1 Activities of trusted third-party archive service provider

Rules applying to internal solutions apply equally to third parties performing electronic archival services. When placing archives in the custody of a trusted third-party archival service, the organization shall check that the techniques and the procedures used ensure security, integrity and long-term preservation of the electronic documents, and that all instructions are traced with related attestations. Annex C presents principles for suggested general service conditions.

Before any transfer of archives to a trusted third party, checks shall be made to ensure that:

a) the third party is able to comply with the requirements specified in this part of ISO 14641;

b) the archival policy used by the third party is compliant with the policy of the organization;

c) security procedures of the third party are compliant with those of the organization.

The third party can either:

— ensure archival of electronic documents (reception and recording of all electronic documents, recording of electronic document archival operations and storage and related metadata), carry out conversion operations, implement replication procedures, ensure access and restitution of documents; or

— store only digital seals of the documents (reception, checks and recording of document-related digital seals, recording of operations), while the storage and preservation of electronic documents corresponding to these signatures remains under the responsibility of the client (originator) organization.

In both cases, the third party shall produce attestations of its activity. The type and frequency of transmission of these attestations from the third party to the client (originator) shall be specified in each third-party contract.

The third party shall keep copies of these attestations in compliance with the specifications of this part of ISO 14641.

In addition to the implementation of an information system compliant with this part of ISO 14641, the third party shall:

1) ensure unique and trustworthy identification for each of its clients;

2) guarantee the confidentiality of the documents and metadata in custody, in particular using an information system implemented in such a way that it will not be possible for a client of the third party to read, write, modify or delete any document of another client of the third party;

3) provide attestations of deposit for each operation;

4) carry out all document deletions after notification and, on completion, provide appropriate attestations;

5) provide an archival lifecycle audit trail for each client that could be produced as evidence in case of dispute.

Exchange of data between the organization and the third party shall be protected by adequate means, i.e. strong authentication, encryption, integrity control.

The third party shall certify that it will make no analysis or processing (e.g. format conversion) of electronic documents in its custody, unless explicit demand has been made by its client (originator).

For reasons of confidentiality, prior encryption of documents and, if appropriate, of metadata can be deemed necessary by an organization. In this case, search criteria for access to the documents might be limited.

13.2 Service contract model

13.2.1 Service contract

The following issues shall be covered in a services contract with any trusted third-party archiving service provider:

a) reference to this part of ISO 14641 with specification of requirements covered;

b) reference to the archival policy;

c) description of archival procedures;

d) description of information system infrastructure;

e) procedures to access information system operations logs;

f) techniques used by the third party to ensure confidentiality of data of the organization;

g) methods and means used for the deposit of electronic documents and their metadata by the client;

h) methods and means taken to ensure, if applicable, format conversion;

i) transportation (physical transfer) procedures of documents, if applicable;

j) insurance policies contracted by the third party covering any activity-related damages.

Even though the terms of the service contract are freely entered into between parties, the content of 13.2.2 to 13.2.13 shall be included.

13.2.2 Service contract duration

The duration of the contract with the third party shall be specified, together with the renewal and termination conditions.

13.2.3 Preservation period

The third party shall commit to the application of the specified preservation period as far as is permitted by the ongoing contractual relationship. The third party shall be able to demonstrate a contractual and technical ability capacity for the restitution and interoperability of its solution in order to ensure the preservation of documents for the agreed duration.

13.2.4 Quality of service

The third party shall commit to a certain level of quality of service and customer support. This commitment concerns levels of availability for the deposit of and access to the archives, possibly associated with penalty clauses when contractual conditions are not fulfilled.

13.2.5 Security and data protection

The third party shall:

a) keep all electronic documents confided by the client (originator) in custody for the contracted period and in the agreed form and formats;

b) guarantee the security and integrity of the electronic documents;

c) commit to perform all media migrations that might be needed to ensure the electronic documents' legibility;

d) provide a secured access service to all objects in custody;

e) maintain an audit trail of all operations related to the execution of services specified by the contract;

f) guarantee the security and integrity of archives' lifecycle and events logs.

13.2.6 Information and counsel

The third party shall inform its client (originator) of the need to maintain compatibility between the client's own information systems and those objects held in custody on the client's behalf. The third party might need to propose additional services to deal with this.

The third party shall inform the client of any conversion operations or of technical changes to the information systems used and of any impact this might have on availability or compatibility with client hardware, or to the exchange of, or preservation of, data in custody.

13.2.7 Transfer and continuity

If a client's electronic documents in custody are transferred to another third party, this entity shall be able to ensure, both during and after the transfer operation, that the documents retain their fundamental properties. This means:

— the other third party shall ensure the full integrity and complete transfer of all archives and all related data it has held in custody;

— in all circumstances, the other third party shall keep information and technical data in such a way that its client, or any party designated by its client, can recover it and do so in a reasonable length of time.

13.2.8 Transferability

On termination of the contract, or if the third party ceases operations, the third party shall be able to return all electronic documents and related elements completely and in the same technical condition they were at the time of reception in the information system. The third party shall not retain any copy of the returned documents.

Return of audit trails/logs shall be specified.

This transferability provision shall allow a client to preserve its independence with regard to the third party, benefiting from a contractual guarantee that the external service can be transferred either to another third party or returned to an internal information system.

This provision shall include, at least:

a) the use by the third party of market standard and state-of-the-art technical tools (architecture, hardware and software, protocols, etc.);

b) the organization of the transfer of the documents either to the client's internal information system (return) or to another third party;

c) the deposit of information and technical data, so that it can be recovered, to a location or by means accessible to its client or any party designated by its client;

d) the cost of the reversibility;

e) the time necessary to perform all reversibility operations from time of request;

f) the regular upkeep of all elements related to reversibility.

13.2.9 Restitution

On termination of contractual preservation obligations, the third party shall undertake to return to its client all archives and shall not keep any copy of them. Nonetheless, if the client specifically makes the request, its archives could continue to be preserved by the third party for an additional period.

13.2.10 Confidentiality and private data

The third party shall guarantee the confidentiality of information it has been trusted with and any other information which might have been made known to it during its contractual relation with its client.

This information could come from access to, or from operations on, documents which it has held in custody, or from its knowledge of the information systems of the organization, whether this knowledge results from its own observations or was provided by its client.

The third party shall take all necessary measures to ensure confidentiality of information that it could become aware of during maintenance activities.

Such information should only be communicated to persons designated by the client, with the exception of situations where it is legally binding to communicate this information to another party.

13.2.11 Professional insurance

The third party shall contract insurance to cover all risks related to its civil liability. This insurance shall provide a financial guarantee relative to the level of duties.

The third party shall maintain this insurance for as long as the service contract applies.

The third party might seek additional insurance protection against information system failure.

13.2.12 Subcontracting

The client shall be informed when the third party plans to use subcontracted services. In this case, the third party remains liable for services provided to the client.

13.2.13 Assessment

The provision related to assessment audits shall conform to the requirements of this part of ISO 14641 (see Clause 12).

14 Service providers

14.1 General

This Clause deals with archival solutions for which some services are provided by subcontractors other than trusted third parties. Annex C presents principles for suggested general service conditions.

The organization implementing the information system service remains liable for the whole system and shall ensure that all services provided by subcontractors comply with the requirements of this part of ISO 14641 according to the duties they are charged with.

The subcontractor selected shall be given a specifications document by an authorized person, defining the requirements. The subcontractor shall commit to these specifications.

Procedures and operations performed by the subcontractor shall be systematically checked and inspected on a regular basis.

14.2 Subcontractor agreement

Before employing the services of a subcontractor, it shall be confirmed that:

— the subcontractor is able to comply with the requirements of this part of ISO 14641 for the services to be provided;

— the subcontractor's procedures comply with the archival policy of the originator;

— the audit trail data produced by the subcontractor is usable on the originator's information system;

— the subcontractor's security policies are consistent with those of the originator.

14.3 Contract with subcontractor

The contract shall include at least the following information:

a) reference to this part of ISO 14641, i.e. ISO 14641-1:2011;

b) description of the procedures used;

c) description of the infrastructure used in relation to the service provided;

d) criteria used for quality control;

e) access to the subcontractor's information system events logs;

f) measures taken to ensure confidentiality and security of data in custody;

g) techniques and media used for the transfer of electronic documents and related metadata between the originator and the subcontractor;

h) techniques used for format conversion, if applicable;

i) provisions for document transfer, if applicable;

j) subcontractor insurance policies covering work-related damages.

14.4 Data transfer over telecommunications networks

When open networks are used to transfer documents between the owner and subcontractor, appropriate techniques for authentication, data integrity and confidentiality shall be used.

Annex A
(informative)

Archival policy

An archival policy describes in legal, functional, operational, technical and security terms the requirements for an internal or external information system, including the aims, targets and commitments of the system.

It should specify the following details.

a) Services provided to depositors and users for deposit or restitution of an archive, including scope of services, levels of service, archival types, electronic document formats, transmission conditions, transfer volumes, frequency of deposits, etc.

b) Obligations incumbent on all parties, primarily on the archival service itself. The obligations regarding other parties should at least indicate the minimum requirements for implementing archival services that conform to the archival policy.

c) Features of operations implemented in order to provide these services (deposit, storage, etc.) and related organization of operations (links between operations, data exchange, etc.).

d) Applicable rules of security according to each level of service and function, based on organizational, practical and technical considerations.

An archival policy is above all a general functional framework and, as such, should be independent from specific techniques used for the purposes of implementing particular operations.

An archival policy is a document that provides all parties involved (internal or external to the service) a clear description of the archival service's commitments. This will entail practical considerations for execution and delivery, including:

— archive deposit;

— identification and authentication of archive source;

— archive accessibility;

— retrieval and display of archives;

— restitution of archives;

— integrity of archives;

— legibility of archives;

— long-term preservation of archives;

— traceability of operations of deposit, restitution and destruction;

— production of attestations;

— business continuity and/or disaster recovery from accidental or malicious causes;

— voluntary destruction of archive.

Annex B
(informative)

Declaration of archival practices

A declaration of archival practices explains the techniques and processes implemented to meet the security targets of the archival policy.

A declaration of archival practice should describe how the archival service of the organization, and/or third-party archive service provider, complies with archival policy requirements in relation to aspects of environment, material, processes, operations and techniques.

A declaration of archival practices should describe:

— the operational processes of the implemented archival service; and

— the security rules described in the archival policy, both in terms of operational security characteristics relative to various components of the archival service and of those needed for the implementation of these characteristics.

These standards and rules should be clearly described in the declaration of archival practice, especially if they are particular to the archival service itself. This declaration could refer to a more general security policy document covering the information system, if appropriate.

The declaration of archival practice should at least include a full and complete description of the practices and should establish the relationship between the rules described in the archival policy to which the declaration refers and to the standards and operational practices.

While an archival policy is established independently of the particular aspects of the operational environment of an information system, a declaration of archival practice is written with regard to the organizational structure, operations processes and material environment of the archival service of the organization or third-party archive service provider.

A declaration of archival practice is always provided by the supplier of the service, i.e. the archival service of the organization or third-party archive service provider.

A declaration of archival practice is in principle a confidential internal document regarding only the archival service. However, to complete the archival policy, an archival service could issue extracts of its declaration of archival practice.

A declaration of archival practice describes how the archival service of the organization and/or third-party archive service provider is able to perform its duty satisfactorily. This should make it particularly useful during any assessment as it will facilitate the work of the auditor and reduce audit time.

Annex C
(informative)

General service conditions

Users of archival services may only have access to the organization's archival policy. It may be difficult for these users to interpret this information.

Accordingly, it would be useful to provide users with a complementary simplified document, which could help in the clarification and understanding of the essential information they would need to know in order to make the informed decisions that they are researching.

General service conditions should contain references to available user manuals. In order to remain clear and intelligible, these manuals should describe only those functions necessary for supported operations, although they could make reference to more general manuals if this were considered to be useful.

The archival services of the organization and/or of a third-party archive service provider should make its general service conditions available to users.

Bibliography

[1] ISO 6196-8, *Micrographics — Vocabulary — Part 8: Use*

[2] ISO 10196, *Document imaging applications — Recommendations for the creation of original documents*

[3] ISO 12029, *Document management — Machine-readable paper forms — Optimal design for user friendliness and electronic document management systems (EDMS)*

[4] ISO 14721, *Space data and information transfer systems — Open archival information system — Reference model*

[5] ISO 15489-1, *Information and documentation — Records management — Parts 1: General*

[6] ISO/TR 15489-2, *Information and documentation — Records management — Part 2: Guidelines*

[7] ISO/TR 15801, *Document management — Information stored electronically — Recommendations for trustworthiness and reliability*

[8] ISO 19005 (all parts), *Document management — Electronic document file format for long-term preservation*

[9] ISO/TR 22957, *Document management — Analysis, selection and implementation of electronic document management systems (EDMS)*

[10] ISO/IEC 13346 (all parts), *Information technology — Volume and file structure of write-once and rewritable media using non-sequential recording for information interchange*

[11] ISO/IEC 13490 (all parts), *Information technology — Volume and file structure of read-only and write-once compact disk media for information interchange*

[12] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[13] IEC 61000-4 (all parts), *Electromagnetic compatibility (EMC) — Part 4: Testing and measurement techniques*

[14] ETSI TS 101 733, *Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats*, European Telecommunications Standardization Institute

[15] ETSI TS 101 903, *Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)*, European Telecommunications Standardization Institute

[16] MoReq2, *Model Requirements for the Management of Electronic Records*, available at www.moreq2.eu

ICS 37.080

Price based on 38 pages