International Standard

ISO 15801

Document management — Electronically stored information — Requirements and guidance for trustworthiness and reliability

Gestion documentaire — Informations stockées électroniquement — Exigences et recommandations pour la fiabilité et la sécurité

First edition
2026-05

Reference number
ISO 15801:2026(en)

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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

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

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

This document was prepared by Technical Committee ISO/TC 171, *Document management applications*, Subcommittee SC 1, *Quality, preservation and integrity of information*.

This first edition of ISO 15801 cancels and replaces ISO/TR 15801:2017, which has been technically revised. The main changes are as follows:

— update from a Technical Report to an International Standard.

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

Introduction

Information is an organizational asset that should be appropriately managed throughout its lifecycle. Ensuring that the organization is able to demonstrate the trustworthiness and reliability of electronically stored information (ESI) is a key consideration. Failure to do so can result in non-compliance, loss of evidential value for information used in business, dispute resolution or legal proceedings.

This document specifies how ESI can be managed by an organization using processes and systems, thus enabling the organization to demonstrate the trustworthiness and reliability of the ESI throughout its lifecycle.

NOTE These processes and systems are sometimes referred to as an information management system.

This document is intended for use in business, compliance, legal or other dispute resolution purposes, where the retained ESI needs to be relied upon to be exactly what it purports to be. This document is intended to be used by:

— managers and professionals involved in management and governance of data, information, records, knowledge, digital preservation or e-discovery;

— designers, vendors and operators of the systems and processes that create, receive, store, transmit, preserve and dispose of ESI.

It would also benefit the academic community and general public.

Where an organization implements the requirements in this document, it is anticipated that the weight of evidence of ESI managed by the systems and processes will be maximized by ensuring its trustworthiness and reliability. This is likely to reduce the effort and cost involved in dispute resolution, as the resolution process will place less emphasis on the trustworthiness or reliability of disclosed ESI. It is also likely that organizations will minimize their risks concerning the credibility of ESI retained for the long term.

ESI originates from many sources. This document covers ESI in any form, from traditional scanned images, word-processed documents and spreadsheets to the more modern forms which include email, web content, instant messages, computer-aided design (CAD) drawing files, blogs, wikis, audio files, pictures and video. Also included is ESI stored in databases, Internet of Things (IoT) systems, distributed ledger technology (including blockchain systems) and other storage systems, including the use of cloud storage.

When ESI preservation is considered, the requirements of ISO 14641 can be used in conjunction with this document.

Document management — Electronically stored information — Requirements and guidance for trustworthiness and reliability

1 Scope

This document specifies requirements for and guidance on the implementation and operation of processes and systems to manage, store and provide access to electronically stored information (ESI) in a trustworthy and reliable manner. Such ESI can be of any type, including "page based" information, information in databases and audio/video information.

This document is intended for any organization that uses processes and systems to store trustworthy ESI over time. Such processes and systems incorporate policies, procedures, technology and audit requirements that ensure that trustworthiness of the ESI is maintained.

This document does not cover processes and systems used to evaluate whether ESI can be considered trustworthy before it is stored or imported into the system. However, it can be used to demonstrate that, once the electronic information is stored, output from the system will be a true and accurate reproduction of the ESI.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 12651 (all parts), *Electronic document management — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12651-1, ISO 12651-2 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
digital seal
data in electronic form which is attached to or logically associated with other data in electronic form to inform on the latter's origin and integrity

3.2
electronically stored information
ESI
information of any kind and from any source, whose temporal existence is evidenced by being stored in or on any electronic medium

Note 1 to entry: ESI includes traditional email, memos, letters, spreadsheets, databases, office documents, presentations and other electronic formats commonly found on a computer. ESI also includes system, application and file-associated metadata such as timestamps, revision history, file type, etc.

Note 2 to entry: Electronic medium can take the form of, but is not limited to, storage devices and storage elements.

3.3
information type
groups of related information

Note 1 to entry: In specific applications, "groups" can be identified as "sets", "files", "collections" or other similar terms.

EXAMPLE Invoices, financial documents, data sheets, correspondence.

3.4
trustworthiness
ability to demonstrate authenticity, integrity and availability of electronically stored information over time

4 Processes and systems

4.1 General

Information is one of the most important assets that any organization has at its disposal. Everything an organization does involves using information in some way. The quantity of information can be vast and there are many different ways of representing and storing it. The value of information used and the manner in which it is applied and moved within and between organizations can determine the success or failure of those organizations.

Information, like any other asset, should be classified, structured, validated, valued, secured, monitored, measured and managed efficiently and effectively.

Where processes and systems manage ESI that may be used as evidence in any legal or business process, the appropriate legal advisors should be consulted to ensure that compliance with relevant legal or regulatory requirements is demonstrable. As legal and regulatory requirements vary from country to country (and sometimes within a country), legal advice should cover all relevant jurisdictions.

4.2 Scope of the ESI system

The organization shall determine the scope and requirements for the ESI system with respect to trustworthiness and reliability.

All ESI used by an organization that is within the scope of the ESI system should be classified into information types. This classification should be used in the creation of policy statement(s).

NOTE For further information on classification, see the ISO 4669 series.

It is possible that the policy statements described in 4.6 do not cover all the different types of ESI that the organization uses. The ESI that will be included in its scope should be identified and grouped into types, with the policy for all ESI within a type being consistent. Where a retention schedule and disposal procedures (see 7.19) exist, it can be appropriate to use the same ESI type groups.

When determining this scope, the organization should consider:

a) the results of the risk management process (see 4.3);

b) the requirements for ESI management (see 4.4); and

c) information classification systems in use (see 4.5).

The scope should be available as part of the policy statement(s).

In many organizations, the trustworthiness and reliability of ESI can only be of importance to part of the overall ESI asset. Individual ESI assets should be identified and a decision should be taken as to whether each should be included within the scope of the related policy.

4.3 Risk management

A risk management process shall be used to identify the scope and requirements that are relevant to the trustworthiness and reliability of ESI.

NOTE 1 The scope and requirements can typically cover the following:

a) the size and complexity of the organization;

b) the level of business risk attached to the inability to demonstrate trustworthiness and reliability of ESI;

c) drivers for business efficiency improvements;

d) specific stakeholder requirements; and

e) the existing technology and infrastructure systems.

NOTE 2 The risk management processes defined in ISO 31000 can be appropriate.

NOTE 3 In order to define and assess the security risks to which ESI is exposed, it can be useful to use a risk analysis method such as that defined in ISO 27005.

4.4 ESI management requirements

When determining ESI management requirements, any applicable legal and regulatory requirements, duty of care expectations, contractual obligations, business requirements and ESI stewardship throughout the ESI lifecycle shall be taken into account. These requirements should cover:

a) stakeholders that are relevant to the trustworthiness and reliability of ESI;

b) the requirements of these stakeholders relevant to that ESI; and

c) the requirements for information stewardship within the organization.

The requirements of each stakeholder should be taken into consideration when producing policy statements (see 4.6).

Information stewardship should be managed by the identification of information asset owners who are typically those responsible for the processes that manage the ESI asset in question.

4.5 Information classification

In some applications, it is appropriate to implement an ESI classification system. Typically, ESI classification systems are used to indicate the accessibility of particular documents to workers and other individuals. In government and other public bodies, this is often indicated by the use of security labels such as “top secret”, “classified” or “publicly available”. In the private sector, ESI classification schemes can be aligned to departmental requirements (such as accounts, credit control or customer services).

The organization shall determine whether to implement an information classification, marking and handling scheme (ICMH) and, if it is decided not to implement an ICMH scheme, the organization shall document the decision and rationale.

NOTE For further information on information classification, marking and handling (ICMH), see ISO 4669-1.

In the event of the organization deciding to implement an ICMH scheme, the structure and operation of that scheme shall be included in the organizational documentation (see 7.1) and shall be retained for at least as long as any ESI utilizing the ICMH scheme is retained.

4.6 Policy requirements

This clause describes documentation that states the organization’s policy for the management of ESI. Additionally, this clause provides guidance to organizations with respect to the level of documentation required to enable an organization to clearly establish how the ESI contained in a trusted system is reliable,