TECHNICAL REPORT

ISO/TR 15801

Third edition
2017-05

Document management — Electronically stored information — Recommendations for trustworthiness and reliability

Gestion de document — Information stockée électroniquement — Recommandations pour contribuer à l'intégrité et à la fiabilité des informations stockées

Reference number
ISO/TR 15801:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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 documents 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).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on 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 the following URL: 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 third edition cancels and replaces the second edition (ISO/TR 15801:2009), which has been technically revised.

Introduction

This document defines recommended practices for electronic storage of business or other information in an electronic form. As such, complying with its recommendations is of value to organizations even when the trustworthiness of the stored information is not being challenged, especially in jurisdictions with e-discovery legislation.

Information originates from many sources. This document covers information in any form, from the traditional scanned images, word processed documents and spreadsheets to the more "modern" forms which include e-mail, web content, instant messages, CAD drawing files, blogs, wikis, etc. Also included is information stored in databases and other data storage systems. Recommendations in this document can be useful in systems that use local and/or cloud storage.

Users of this document should be aware that the implementation of these recommendations does not automatically ensure acceptability of the evidence contained within the information. Where electronically stored information (ESI) might be required in court or other adversarial situation, implementers of this document are advised to seek legal advice to ascertain the precise situation within their relevant legal environment.

This document describes means by which it can be demonstrated, at any time, that the information created or existing within an information management system has not changed since it was created within the system or imported into it.

Regardless of the original format, it will be possible to demonstrate that information stored in a trustworthy information management system can be reliably reproduced in a consistent manner and accurately reflects what was originally stored without any material modification.

Alternative versions of the information in a document might legitimately develop, e.g. revision of a contract. In these cases, the new versions are treated as new documents. The same principle can be applied when a significant change is made to a document in a workflow environment.

Information technology based systems can store, in an electronic form, both documents and records. This document describes means for storing all types of ESI in a trustworthy and reliable manner, as part of an information governance strategy. Where records (as defined in ISO 15489-1) are stored, the requirements of this document can be used in conjunction with those specified in ISO 15489-1 to ensure that the policies and procedures described in this document work in conjunction with those specified in ISO 15489-1.

When information preservation is considered, the requirements of ISO 14641 can be used in conjunction with this document. Readers are advised to use this document in conjunction with other local sources, particularly with relevance to governmental and legal requirements in their respective jurisdictions.

Document management — Electronically stored information — Recommendations for trustworthiness and reliability

1 Scope

This document describes the implementation and operation of information management systems that store and make available for use 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 for use by any organization that uses systems to store trustworthy ESI over time. Such systems incorporate policies, procedures, technology and audit requirements that ensure that trustworthiness of the ESI is maintained.

This document does not cover processes used to evaluate whether ESI can be considered to be trustworthy prior to it being 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 created and/or imported.

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 (all parts) and the following apply.

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

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

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

3.1
electronically stored information
ESI
data or 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 e-mail, 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.

[SOURCE: ISO/IEC 27040:2015, 3.16]

3.2
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.

3.3
trustworthy
ability to demonstrate authenticity, integrity and availability of *ESI* (3.1) over time

3.4
trusted system
information technology system with the capability of managing *ESI* (3.1) in a *trustworthy* (3.3) manner

4 Information management policy

4.1 General

Information is one of the most important assets that any organization has at its disposal. Everything an organization does involve 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, needs to be classified, structured, validated, valued, secured, monitored, measured and managed efficiently and effectively.

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, accurate and trustworthy. Availability of this documentation can also be used to demonstrate that ESI management is part of normal business procedures.

Where an information management system manages ESI that might be used as evidence in any legal or business process, the appropriate legal advisors should be consulted (see 5.4) 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 Information management policy document

4.2.1 Contents

An information management policy document (the policy document) should be produced, documenting the organization’s policy on the storage of ESI, as applicable to the trusted system.

The policy document should contain sections which:

— specify what ESI is covered (see 4.2.2);

— state policy regarding roles and responsibilities for ESI (see 4.2.3);

— state ESI security classification policies (see 4.2.4);

— state policy regarding storage media (see 4.2.5);

— state policy regarding electronic file formats and version control (see 4.2.6);

— state policy for the use of outsourcing (see 4.2.7);

— state policy regarding relevant information management standards (see 4.2.8);

— define ESI retention and disposal policies (see 4.2.9);

— define responsibilities for information management functions (see 4.2.10);

— define responsibilities for monitoring compliance with this policy (see 4.2.11).

The policy document should be approved by senior management of the organization and should be reviewed at regular intervals.

Essential to this implementation of this document is the agreement and implementation of a retention schedule for ESI. Where reference is made to the policy document in the rest of this document, the retention schedule is included in such a reference.

4.2.2 ESI covered

In order to define the organization's information management policy, information should be grouped into types, the policy for all information within a type being consistent. For example, information types can be specified either by reference to application (e.g. financial projections, invoices, customer address list), by association with a specific business process (e.g. applications, complaints, renewals) or by reference to generic groups (e.g. accounting data, customer documents, manufacturing documents).

During the drafting of the policy document, specific information might need to be regrouped to ensure consistency of policy within an information type.

The policy document should list all types of information that are to be stored in compliance with the policy. The policy document should include, as an information type, all information produced, received and stored in compliance with the policy.

4.2.3 ESI roles and responsibilities

The individuals or teams responsible for the management of the ESI should be identified and their roles defined. These roles should include:

— following a systematic approach to ESI management;

— being business focused and aware of the current business requirements;

— being able to communicate at all levels within the organization;

— having a good understanding of risk management in relation to trustworthy ESI.

4.2.4 ESI security classification

In some applications, it may be appropriate to implement an ESI security classification system, typically used to indicate the accessibility of particular information. 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, security classification schemes may be aligned to departmental requirements (such as accounts, credit control or customer services).

The ESI security classification system should be simple to use and should be based on risk, need, priority and the degree of protection appropriate. Excessive classification levels should be avoided.

Where an ESI security classification system is in use, the policy document should include with each information type the relevant classification level.

4.2.5 Storage media

Different types of media have different long-term storage characteristics. Most organizations will manage ESI on a variety of media types: electronic (hard disk drives, cloud storage), paper, microform, optical (write-once and rewritable/erasable) or hybrid types. In some applications, specific pieces of ESI can, throughout their retention period, be stored on different media types.

The organization should have policies regarding the use of specific types of media for different information storage requirements (e.g. access requirements, retention periods and security requirements). These policies should be detailed in the policy document.

The media type on which each information type (see 4.2.3) can be stored should be specified.

Where copies of ESI exist, it might be important to be able to demonstrate that no changes have occurred to any purported copy. In the case of ESI that exist in different versions, for the purposes of this document, each version should be treated as a new source or original ESI.

The policy for the management of copies of ESI should be detailed in the policy document.

4.2.6 Data file formats and compression

The policy document should contain details of the approved data file formats that can be used for each information type.

All ESI managed by information management systems require software for retrieval and display. This software is subject to change, either by the implementation of new releases or by changes to operating systems and/or hardware. By implementing a policy of approved data file formats and compression technologies (where utilized), the necessary data migration or alternative procedures can be implemented satisfactorily to ensure long-term retrieval of the ESI.

Where compression techniques are employed, policy on their use should be documented.

Where multiple versions of ESI can exist, a policy is required which ensures that all relevant versions are managed and their relationship maintained. The policy document should contain details of policy on the management of versions of ESI.

For additional information on this, see 6.5.2, 6.11, 7.10 and 8.2.3.

4.2.7 Outsourcing

The policy document should contain guidelines on the use of outsourcing processes that can be used for each information type. The policy should include the use of specific contract clauses where this is appropriate [in particular, where information about individuals (personal data, PII) is involved]; this can be achieved by the use of standard contract clauses or the use of a draft contract. It may also be appropriate for the policy document to require an appropriate service level agreement to be included in the final contract with the outsource organization.

For additional information, see 6.16.

4.2.8 Standards related to information management

Where the organization operates a quality management system (such as the ISO 9000- series) whose scope includes part or all of the trusted system, all relevant procedural documentation should be included in the quality management system.

Where national or international regulatory requirements are mandatory, or where national or International Standards are applicable, they should be listed and complied with.

4.2.9 Retention and disposal schedules

A retention schedule should be established for each information type.

Retention periods should be agreed by all relevant departments and personnel within the organization. Retention periods should be agreed upon after taking relevant advice to ensure that legal or regulatory issues, or both, are resolved.

All relevant system and procedural documentation that is produced should be covered by the retention schedule.

The retention schedule should include the organization's policy for its periodic review.

The retention schedule should include the organization's policy for the controlled destruction of ESI.

4.2.10 Information management responsibilities

Individual or job function responsibilities for the policy document should be defined in the policy document. Individual or job function responsibilities for each information type should be identified and included in the policy document.

Individual or job function responsibilities should include the need to seek relevant advice when creating or updating the contents of the policy document.

4.2.11 Compliance with policy

Where it is important that compliance with the policy document can be demonstrated, the individual or job function responsibilities for obtaining and maintaining such compliance should be identified and defined.

5 Duty of care

5.1 General

5.1.1 Trusted system

A trusted system is one that ensures that all ESI managed by the system can be considered to be original information, or a true and accurate copy of the original information, regardless of the original format. Trusted systems should include the following as a recommended minimum:

— the creation of at least one copy of the ESI on to a system that protects the ESI from modification, inappropriate additions or deletion throughout its approved lifecycle; this copy needs to be stored and maintained in a safe location that is separate and remote from other copies of the ESI;

— the utilization of hardware and storage media that protect the ESI from modification, inappropriate additions or deletion throughout its approved lifecycle (see also 7.3);

— the ability to verify through independent audit processes of the software, hardware and/or storage media methodology(ies) that the ESI can be rendered accurately throughout its approved lifecycle.

A trusted system utilizes a combination of organizational policies, operational procedures and appropriately installed and managed technologies as described in this document that will enable an organization to demonstrate trustworthiness and reliability.

5.1.2 Controls

It is essential that the organization be aware of the importance of designing and maintaining all aspects of the trusted system and that it execute its responsibilities under the duty of care principle.

To fulfil this objective, the organization needs to:

— establish a chain of accountability and assign responsibility for activities involving management of ESI at all levels;

— be aware of legislative and regulatory bodies pertinent to its business;

— keep abreast of technical, procedural, regulatory and legislative developments by maintaining contact with the appropriate bodies and organizations;

— implement an information security policy.

5.1.3 Segregation of roles

The segregation of roles is a fundamental aspect of duty of care. It provides a check on errors and on the deliberate falsification of ESI (in this respect, separation of roles is particularly important in systems where there is risk of fraud or other malicious action).

There are several aspects of information management where a segregation of roles is considered:

— input reconciliation (see 6.4.3);

— quality control (see 6.4.6);

— data entry (see 6.7);

— information deletion (see 6.12);

— information security (see 5.2).

It is also important to ensure that the physical and managerial segregations that exist around a trusted system are mirrored by the logical access controls within it.

The segregation of roles between initial operations and checking should be reviewed and implemented where appropriate.

5.2 Information security management

5.2.1 Information security policy

All ESI, irrespective of the media on which it is stored, is vulnerable to loss or change, whether accidental or malicious. To protect ESI, security measures need to be developed and implemented to reduce the risk of a successful challenge to its trustworthiness. These security measures need to be aligned to any ESI classification categories that are used.

Traditionally, information security is often considered a matter of confidentiality, to ensure that information is not accessible outside the requirements of the organization. However, while this is important (in some cases vital) to the operation of the organization, it is not the most important security issue relevant to this document. Trustworthiness relates to the ESI's characteristics of authenticity, integrity and availability.

A key objective of the information security policy is to ensure the protection of the trustworthiness of ESI. When developing security measures, it is necessary to compare the risk of trustworthiness being compromised or challenged with the cost of implementation of such measures. Security measures need to include backup and other copies of ESI, as their trustworthiness is of importance in circumstances where they have been used as replacements for live ESI.

Also of importance is availability (which includes the ability to read, search and retrieve information). In some cases, it might be necessary to be able to demonstrate that all information on a specific topic is available for review at any time. In this category, topics such as indexing accuracy and business continuity planning are important.

Security is not singularly a concern of information management systems. Security and availability of the operating environment (including buildings, temperature controls, network links, etc.) and the auditable implementation of procedures by all staff are both key elements.

The organization should adopt an information security policy, covering all elements of the trusted system.

Where the organization has an information security policy for other systems, then the use of the trusted system should be incorporated within its scope.

The information security policy document should contain, as a minimum, the following:

— statement of management objectives in respect of security;

— specific policy statements;

— requirements for different ESI classification categories;

— definition and allocation of information security responsibilities;

— policy for dealing with breaches of security;

— policy regarding compliance with relevant legislation, regulation and/or contractual requirements;

— policy regarding compliance with relevant standards.

The information security policy document should be approved by the organization's senior management. That approval should be documented.

The organization should agree and document appropriate levels of security for managing its ESI, in compliance with its information security policy document.

Consideration should be given to compliance with ISO/IEC 27001. With reference to the trusted system, the requirements of this document should be taken into consideration when developing the required controls for compliance with ISO/IEC 27001.

5.2.2 Risk assessment

Security measures are often developed using an ad hoc approach, reacting to security incidents or to available 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 should 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 needs to include vulnerability risk factors consistent with the type of media being used (e.g. WORM or rewritable).

The impact on the risk analysis results should be reviewed in relation to all the different types of storage media in use.

Once the risk analysis has been completed, it needs to 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 need to be taken into consideration during the review process.

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

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

For further information, see ISO/TR 18128 and ISO 31000.