TECHNICAL REPORT

ISO/TR 15801

First edition
2004-02-01

Electronic imaging — Information stored electronically — Recommendations for trustworthiness and reliability

Images électroniques — Stockage électronique d'informations — Recommandations pour les informations de valeur et leur fiabilité

Reference number
ISO/TR 15801:2004(E)

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.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

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/TR 15801 was prepared by Technical Committee ISO/TC 171, *Document management applications*, Subcommittee SC 3, *General issues*.

Introduction

Increasingly, information that has been created, captured and stored electronically is used as evidence of business activities. Such evidence might be required in contract discussions, or in courts of law. This Technical Report defines recommended practices for electronic storage of business or other information in image form. As such, complying with its recommendations is of value to organizations even when the trustworthiness of the stored information is not being challenged.

Users of this Technical Report should be aware that the implementation of these recommendations does not automatically ensure acceptability of the evidence encapsulated by the information. Where stored electronic information may be required in court, implementers of this Technical Report are advised to seek legal advice to ascertain the precise situation within their relevant legal environment.

This Technical Report describes means by which it may be demonstrated, at any time, that the contents of a specific electronic image file created or existing within a computer system have not changed since it was created within the system or imported into it. Where such a data file contains a digitized image of a physical source document, it will be possible to demonstrate that the digitized image is a true facsimile of that source document. The issue being addressed is essentially one of authentication.

Other versions of the information may legitimately develop; e.g. revision of a contract. In these cases the new versions are treated as new image files.

The same principle can be applied when a significant change is made to a document in a workflow environment.

This Technical Report describes procedures whereby an electronic copy may be demonstrated to be a true copy of the original, whether that original was itself an electronic data file or a physical source document.

The recommendations in this Technical Report are a mixture of items that are broad and general and items that are specific and detailed. Readers are advised to use this Technical Report in conjunction with other local sources, particularly with relevance to governmental and legal requirements in their respective jurisdictions.

Organizations that implement most of the recommendations described in this Technical Report will be in a good position to be able to demonstrate authenticity. However, there may be good economic reasons where a particular recommendation is not implemented. In such situations, the risk taken by such non-implementation decisions should be assessed.

Electronic imaging — Information stored electronically — Recommendations for trustworthiness and reliability

1 Scope

This Technical Report describes the implementation and operation of information management systems which store information electronically and where the issues of trustworthiness, reliability, authenticity and integrity are important. The whole life cycle of a stored electronic document is covered, from initial capture to eventual destruction.

This Technical Report is for use with any information management system, including traditional document imaging, workflow and COLD/ERM technologies, and using any type of electronic storage medium including WORM and rewritable technologies.

Image files may potentially contain any type of data: for example, correspondence, forms, drawings. This Technical Report covers all such image files, whether created and/or imported directly or through a network, from the time at which the system assumes control of the image file.

This Technical Report does not cover processes used to evaluate the authenticity of information prior to it being stored or imported into the system. However, it can be used to demonstrate that output from the system is a true reproduction of the original document.

Where in this document the term *system* is used, it should be taken as meaning the *information management system* that is being reviewed, unless otherwise stated.

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 9000 (all parts), *Quality management and quality assurance standards*

ISO/TR 12037:1998, *Electronic imaging — Recommendations for the expungement of information recorded on write-once optical media*

ISO 12651:1999, *Electronic imaging — Vocabulary*

ISO 12653-2:2000, *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 12651 and the following apply.

3.1
information type
groups of related documents

NOTE In specific applications, “groups” may be identified as “sets”, “files”, “collections” or other similar terms.

EXAMPLES Invoices, financial document, data sheets, correspondence.

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 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 may 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 information management policy. Availability of this documentation will demonstrate that information management is part of normal business procedures.

Where a system stores records, compliance with ISO 15489 should be considered. Such compliance will ensure that many of the elements of this Technical Report will be implemented. Where a system stores information that may be used as evidence in court, your legal advisors should be consulted (see 5.4) to ensure that you comply with relevant legal or regulatory requirements. As legal and regulatory requirements vary from country to country (and sometimes within a country), the legal advice you obtain 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 information management and storage, as applicable to the information management system.

The Policy Document should contain sections which:

— specify what information is covered (see 4.2.2);

— state policy regarding storage media (see 4.2.3);

— state policy regarding image file formats and version control (see 4.2.4);

— state policy regarding relevant information management standards (see 4.2.5);

— define retention and destruction policies (see 4.2.6);

— define responsibilities for information management functions (see 4.2.7);

— define responsibilities for monitoring compliance with this policy (see 4.2.8).

The Policy Document should be approved by senior management of the organization, and should be reviewed at regular intervals.

Essential to this Technical Report is the agreement and implementation of a Retention Schedule for stored information. Where reference is made to the Policy Document in the rest of this Technical Report, the Retention Schedule is included in such a reference.

4.2.2 Information 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 may be specified either by reference to application (e.g. financial projections, invoices, customer address list), or to generic group (e.g. accounting data, customer documents, manufacturing documents).

During the drafting of the Policy Document, specific information may need to be moved from one type to another to ensure consistency of Policy within an information type.

The Policy Document should list all types of information which are to be stored. The Policy Document should include as an information type all documents produced in compliance with the Policy.

4.2.3 Storage media

Different types of media have different long-term storage characteristics. Most organizations will store information on a variety of media types: paper; microform; electronic (write-once and rewritable/erasable). In some applications, specific pieces of information may, throughout its retention period, be stored on different media types at different times.

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.

NOTE In some countries, only certain media types can be used where stored information may be required as evidence. For example, in France, rewritable media cannot be used in evidential matters.

The media type on which each information type (see 4.2.2) may be stored should be specified.

It should be possible, where copies of image files exist, to be able to trace back to the earliest such files, in order to be able to determine that no changes have occurred to any purported copy. Note that, in the case of files that exist in different versions, each version should be treated as a new source or original file for the purposes of this Technical Report.

The policy for tracking copies of image files should be detailed in the Policy Document.

4.2.4 Image file formats

The Policy Document should contain details of the approved image file formats that may be used for each information type.

All information stored on a computer system requires 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 storage formats, the necessary data migration or alternative procedures can be implemented satisfactorily to ensure long-term retrieval of the stored information.

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

Where multiple versions of a document may be stored, a policy is required which ensures that all relevant versions are stored, and their relationship maintained. The Policy Document should contain details of policy on the storage of versions of documents.

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

4.2.5 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 information management system, then all relevant procedural documentation should be included in the quality system.

Where National or International regulatory requirements are mandatory, or where National or International Standards are applicable, they should be complied with.

4.2.6 Retention schedule

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 information.

4.2.7 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.

4.2.8 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 Controls

It is essential that the organization is aware of the value of information that it stores, and executes its responsibility 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 electronic information 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.

5.1.2 Separation of roles

The separation of roles is a fundamental aspect of duty of care. It provides a check on errors and on the deliberate falsification of records (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 separation of roles is considered:

— input reconciliation (see 6.4.3);

— quality control (see 6.4.6);

— data entry (see 6.6.2);

— information deletion (see 6.9);

— information security (see 5.2).

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

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

Traditionally, information security is considered a matter of confidentiality, to ensure that information is not accessible outside the requirements of the organization. However, whilst this is important (in some cases vital) to the operation of the organization, it is not the most important security issue relevant to this Technical Report.

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

Also of importance is availability. In some cases, it may 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 key.

Security is not singularly a concern of computer 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 information management system.