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

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

Reference number
ISO/TR 15801:2017(E)

© ISO 2017

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

COPYRIGHT PROTECTED DOCUMENT

© ISO 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
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

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

© ISO 2017 – All rights reserved

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

© ISO 2017 – All rights reserved

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

© ISO 2017 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

© ISO 2017 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

© ISO 2017 – All rights reserved

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

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]

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

© ISO 2017 – All rights reserved

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);

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

© ISO 2017 – All rights reserved

- 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.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

© ISO 2017 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

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.

© ISO 2017 – All rights reserved

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

5.2.3 Information security framework

A management framework should be established to initiate and control the implementation of information security within the organization. The framework should have as its objectives:

- approval and review of the information security policy;
- monitoring of threats to information security;
- monitoring and review of security breaches;
- approval of major initiatives to enhance information security.

5.3 Business continuity planning

From time to time, problems arise with trusted systems which require emergency procedures to be implemented to recover from the problem. Such procedures might involve the temporary use of additional or third-party resources. In order to ensure that the trustworthiness of ESI is not compromised during these operations, an agreed and approved business continuity plan (sometimes known as a disaster recovery plan) should be implemented.

Procedures to be used in cases of major equipment, environmental or personnel failure should be developed, tested and maintained. Such procedures should ensure that the trustworthiness of ESI is not compromised during their implementation.

For further information, see ISO 22301 and ISO 22313.

5.4 Consultations

The implications of using trusted systems can be significant to other organizations, such as:

- regulatory bodies;
- government bodies;
- external audit bodies;
- legal advisors (such as the organization's lawyers).

The organization should consult with relevant organizations that are concerned with the trustworthiness of ESI prior to implementing the information management policy document.

These can include the following:

- national and international law;
- industry sector;
- community;
- organization;
- department;
- individual.

The organization should consult with relevant organizations prior to implementing the information management policy document.

These consultations can include the following topics:

- legal issues;

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

© ISO 2017 – All rights reserved

- government regulations;
- financial regulations (such as payment of taxes);
- special regulations (applicable to particular sectors).

The results of all consultations, including actions agreed, planned or implemented, should be referenced or included in the policy document.

Where appropriate regulations and/or laws exist, they should be complied with.

The policy document should state whether all or part of any relevant national or International Standards should be complied with.

Where the organization complies with relevant national or International Standards, such compliance should include the trusted system.

6 Procedures and processes

6.1 General

This clause deals with procedures relating to the operation of a trusted system.

6.2 Procedures manual

6.2.1 Documentation

The organization should maintain a procedures manual for each trusted system. Where, in this subclause, documentation is required, this documentation can either be included in the procedures manual or referenced by it. This manual may include references to other controlled documentation as appropriate.

The relevant procedures detailed in, or referenced by, the procedures manual should be readily accessible to all appropriate users of the system.

6.2.2 Content

The procedures manual should include or reference procedures for the operation of the trusted system and should include the following:

- ESI capture (see 6.3);
- document image capture (see 6.4);
- data capture (see 6.5);
- indexing (see 6.7);
- authenticated output procedures (see 6.8);
- file transmission (see 6.9);
- information retention (see 6.10);
- information preservation (see 6.11);
- information destruction (see 6.12);
- backup and system recovery (see 6.13);
- system maintenance (see 6.14);

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

© ISO 2017 – All rights reserved

- security and protection (see 6.15);
- use of contracted services (see 6.16);
- workflow (see 6.17);
- date and time stamps (see 6.18);
- version control (see 6.19);
- maintenance of documentation (see 6.20).

For convenience, the procedures manual can be maintained as a number of separate physical documents, relating to different information management areas.

Where the organization has multiple trusted systems, the documentation can comprise a single procedures manual or multiple procedures manuals.

6.2.3 Compliance with procedures

In order to be able to comply with the procedures detailed in the procedures manual, staff members need to be aware of them and have the ability to follow them. This situation is frequently achieved by training, either by specific courses or during day-to-day working.

Procedures should be implemented that ensure that all staff members that operate the system adhere to requirements.

6.2.4 Updating and reviews

It is important to ensure that the procedures implemented at any time during the storage life of any specific piece of ESI can be determined. This is achieved by ensuring that the procedures manual is kept up to date and that all previous versions are kept in compliance with the policy document.

Any changes to operational procedures should be documented. This documentation should include details of any change control procedures used and procedures to ensure that the new procedures are implemented.

Where changes are being implemented, they should be checked to ensure that operational requirements and the requirements of the policy document are not compromised.

Superseded versions of the procedures manual should be kept in compliance with the policy document (which includes compliance with the retention schedule).

To confirm that documentation is up to date, regular reviews are necessary. Such reviews might also be necessary where legal or regulatory changes are relevant.

A review should be carried out at least annually to ensure that any changes to procedures or technology are reflected in the procedures manual.

The results of periodic reviews should be documented and approved by the person responsible for the operation of the appropriate part of the system.

6.3 ESI capture

6.3.1 General

Where a trusted system is used for managing ESI, the procedures involved in the capture of the ESI should be documented.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

6.3.2 Creation and importing

ESI can be created within a trusted system, or imported into it. The trustworthiness of the ESI at the time that it is created or imported is of critical importance, as the trusted system will consistently reproduce whatever ESI has been managed.

ESI is typically stored as either images or data. In either form, ESI can be imported into the trusted system in a variety of formats.

Image formats are typically obtained from:

- images such as that captured by cameras;
- automatic facsimile entry (through a fax server);
- capturing screen shots where multiple pieces of information are being displayed simultaneously (also referred to as compound transient documents).

Image formats are typically bit maps of an original analogue document. Details of procedures for capturing analogue documents in image format are discussed in 6.4.

Data formats store information in "native" format, maybe requiring the original software to retrieve the information contained. There are a number of "standard" formats that can be retrieved by many software packages (e.g. text files, comma-separated delimited files). Examples of data formats are:

- office systems such as word processors, spreadsheets, etc.;
- database systems;
- CAD drawings;
- e-mail messages;
- electronic data interchange (EDI) files;
- instant messages;
- XML messages.

In all cases, the information contained can be accessed through the use of an appropriate software application. Details of procedures for capturing analogue documents in data format are discussed in 6.5.

NOTE It is also possible to have ESI in mixed image and data formats (for example, a letter in Word format with an embedded bit-mapped signature).

Where ESI to be managed by a trusted system originates from outside the boundaries of control of the organization employing the trusted system, there might be little or no control over, or knowledge of, the procedures or processes involved in the production or authorization of that ESI. In these circumstances, the organization will need to take care that the ESI is what it purports to be, that it has not been tampered with and that the identity of the originator is genuine. The level of checking of these criteria will depend upon the nature of the particular ESI in question.

Such boundary situations can also exist within an organization. In these circumstances, the part of the organization with the trusted system should not assume that ESI is what it purports to be, simply because it came from another part of the same organization.

6.3.3 Information loss

Where ESI is stored in a trusted system, potentially, there is the possibility of loss of some of the information. For example, when ESI is converted from one format to another, some metadata might be lost.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

Where ESI contains macros or other set of instructions that might affect its information content, care needs to be taken to ensure that all the appropriate information is captured.

Where storage media is changed, physical evidence (such as fingerprints on CD media) might not be reproduced within the ESI. In such cases, the organization should review any potential loss of information and make a decision as to whether this loss is acceptable to the business process. If such a loss is unacceptable, steps should be taken to ensure that all the required information is captured and/or retained.

6.3.4 Metadata

When ESI is created or imported, care should be taken to ensure that all the relevant metadata are also transferred. Care should be taken to ensure that all necessary metadata are captured, to ensure that the ESI has the correct interpretation placed on it.

The content of metadata might need to be reviewed for completeness and appropriateness. The availability of a full metadata set, with an appropriate content, will increase the evidential value of the ESI to which it pertains. The use of an appropriate metadata schema should be considered.

6.4 Document image capture

6.4.1 General

This subclause includes recommendations relating to the procedures relevant to the creation of electronic images from analogue documents. Recommendations in this subclause are for users whose trusted systems include the capture and storage of analogue documents in an electronic form by the use of scanners or cameras. These recommendations cover procedures for:

- preparation of documents;
- document batching;
- photocopying;
- scanning;
- image processing.

See also ISO/TR 13028.

6.4.2 Preparation of paper documents

All paper documents need to be examined prior to the scanning process, to ensure that a successful image is obtained. Attributes such as paper size, weight and binding, paper and print colour can all affect the physical scanning process.

Paper documents should be examined prior to the scanning process to ensure their suitability for scanning. Procedures for this examination process should be documented.

Factors such as their physical state (thin paper, creased, stapled, etc.) and the attributes of the information (black-and-white, colour, tonal range, etc.) should be considered.

Where paper documents are found that are unlikely to be accepted by the scanner, there are a number of techniques that can be used. For example, the original could be photocopied or transparent wallets could be used.

Procedures to be followed for paper documents that can cause scanning difficulties should be documented. When removing staples, clips or other paper document bindings, ensure that no damage is caused to the original that can affect the capture of the information from the document.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

© ISO 2017 – All rights reserved

Where a paper document has physical attachments, for example, stick-on notes, the system should provide facilities for distinguishing these from the document to which they are attached.

This might be achieved, for example, by capturing a separate image of the attachment, with appropriate data to associate it with the source page. If only a single image is captured with the attachment in place, the data might record the fact that there is an attachment. Where there is a risk that an attachment might obscure, or be considered too obscure, information on the paper document, it might be preferable to ensure that an image of the paper document without the attachment is captured.

Where a paper document has physical amendments, for example, white opaque paint, the system should ensure that the presence of such amendments is noted.

Procedures to be followed when scanning multi-page paper documents bound together with staples or clips should be documented.

All pages of multi-page paper documents should be kept together and in the appropriate order before, during and after scanning.

6.4.3 Document batching

Wherever appropriate, paper documents should be grouped into batches for scanning.

This makes it easier to control the paper documents and to be able to perform quality control and other procedures on a sampling basis.

The definition of batch size should be decided on the basis of convenience.

The number of paper documents in a batch will be application-dependent. For example, if the documents are in file covers and the average number of documents per file cover is relatively large, for example, 100 pages, then the documents in a single file cover can constitute a batch. If the file covers contain relatively few documents, for example, on average 10 pages, then a batch can consist of documents from more than one file cover. If the documents are on roll microfilm, the film roll can be a batch.

Choose the batch size so that it is not bigger than can be easily managed, nor so small that checking quality by sampling on a batch basis would result in significant process inefficiencies. Sample size might need to be determined using statistical sampling techniques.

For some applications, a batch cannot be easily defined. In these cases, a batch can be defined as those paper documents input during a specified time period. Thus, for example, a batch could be all documents input during an hour or a day.

For some applications (especially where workflow is implemented) where batching cannot be applied, alternative methods for ensuring that all paper documents are scanned should be established. Such techniques can include the marking of documents after scanning or additional checking of images against the paper originals.

STANDARDSISO.COM Click to view the full PDF of ISO/TR 15801:2017

6.4.4 Photocopying

It might be helpful for some paper documents to be photocopied prior to being scanned. Such documents include the following:

- documents that can be adversely affected by the scanning process, such as damaged or delicate documents;
- documents where there are substantial contrast or density variations over the area of the original and where photocopying demonstrably improves the image quality;
- documents containing paper or ink colours that do not produce legible scanned images;

  NOTE 1 Photocopiers and scanners might respond differently to different colours and it is only in exceptional cases that the technique of photocopying prior to scanning does not produce satisfactory results.

— folded documents that are too large to be scanned as a single full-sized image.

NOTE 2 Photo reductions can be made which are then scanned and/or multiple scanned images can be captured from the original or from photocopies thereof.

Photocopies should be examined to ensure that there is no significant loss of information during this process.

Where paper documents are photocopied prior to the scanning process, the procedures used should be documented in the procedures manual.

Additional quality control procedures should be adopted to ensure that no significant information is lost in the scanning of photocopied paper documents.

If photo reductions are made, checks should be made to ensure that there is no significant loss of detail in the scanned images compared to the paper original caused by the effective resolution of the image (compared to the original) being reduced.

If multiple images are captured, these should be overlapped to ensure that there is no significant loss of information at the edges between adjoining images.

Where an image was made from a photocopy, it should be clear to a user of the image that this was the case. It should also be clear whether the photocopy was made from the paper document during document preparation or whether the paper document was known to be a photocopy. This is to ensure that an image can be correctly identified as a true facsimile of a paper document, even if an intermediate photocopy has been taken as part of the preparation procedures and to distinguish such images from images of photocopies made under unknown conditions.

This can be done, for example, during document preparation, by stamping or marking the document as a photocopy or original photocopy or by electronically marking the image as having been captured from a photocopy, distinguishing between photocopies made during document preparation and paper documents which are known photocopies.

Procedures to be used where it is not known whether a paper document is an original or a photocopy should be documented.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

6.4.5 Scanning processes

Details of procedures used in analogue document scanning should be included in the procedures manual.

Any variations in scanning procedures due to the type of document being scanned should be detailed in the procedures manual.

Such changes might apply to, for example, double-sided versus single-sided paper documents and colour versus black-and-white images.

Procedures should ensure that all paper documents in a batch are fully scanned; no document should be left unscanned.

To check that all paper documents have been scanned, the count of captured documents can be compared with the number of documents in a batch. Where batching is not used, alternative procedures for ensuring that all documents are scanned might be needed.

Where it is important that all pages in a multi-page paper document are scanned, procedures which ensure this should be implemented.

The count of captured images per paper document can be compared with the number of pages (i.e. sides) in each document, taking into consideration any blank page (or other) removal processes. However, errors in manually counting physical paper documents and the pages therein might make such a process ineffectual. It might be satisfactory to implement procedures whereby the probability and risk of any document not being scanned is acceptably small. This risk should be evaluated and, where necessary, procedures should be reviewed against this risk.

Many scanners have automatic paper document feeders that can reliably detect bad feeds, therefore, minimizing the risk that a document might pass through the scanner without being scanned. If such devices are not used, the procedures are required to ensure that the scanner operator has to manually handle every document in order to reduce the probability that any document might not be scanned.

Where it is crucial to ensure that every sheet is scanned, users should consider counting or pre-indexing the paper documents in order to capture accurately the number of pages per document or batch of documents.

Using a double-entry technique can provide extremely high accuracy in the number of pages. These data can subsequently be compared with the scanned page count; any shortfall will indicate either that more than one page has been fed at once or that a page has been misplaced between pre-indexing and scanning.

If a simplex scanner (i.e. one that scans only one side of a paper document at a time) is used to scan double- sided documents, care should be taken to ensure that every double-sided document is reversed and the other side scanned.

If a large paper document is scanned in sections, so that multiple images are captured, these sections should be overlapped to ensure there is no loss of information at the edges between adjoining images.

The scanning system should enable each electronic document to be uniquely identified, in such a way that its identity cannot be changed or removed, except as permitted as described in 7.11.

This unique identity could be a system-generated sequence number that can be used for internal control purposes only.

6.4.6 Quality control

6.4.6.1 Sample set

Procedures are required which reduce the risk of scanned images being of unsatisfactory quality. It will be easier to demonstrate trustworthiness if it can be shown that the images are of good quality and that the scanner was working to agreed standards at the time of scanning.

A sample set of paper documents should be assembled for the purposes of evaluating scanner results against agreed quality control criteria. Documents in the sample set should be representative of the complete set of documents that are to be scanned. Documents in the sample set should include examples of paper documents whose quality is poor relative to those of the majority of the documents.

Quality control criteria can cover:

- overall legibility;
- smallest detail legibly captured (e.g. smallest type size for text; clarity of punctuation marks, including decimal points);
- completeness of detail (e.g. acceptability of broken characters, missing segments of lines);
- dimensional accuracy compared with the original;
- scanner-generated speckle (i.e. speckle not present on the original);
- completeness of overall image area (i.e. missing information at the edges of the image area);
- density of solid black areas;
- colour fidelity.

Quality control criteria for image quality should be realistic given the nature of the source material and the characteristics of the scanning equipment.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

Quality control criteria should be documented for scanned image quality. The criteria should be agreed by all parties, whose use of images is likely to be affected by image quality, including internal and external users.

Quality control criteria should be based upon the sample set of paper documents.

6.4.6.2 Evaluating image quality

Procedures that specify the process used for evaluating image quality on a day-to-day basis should be documented.

Image quality evaluation procedures should include details of the evaluation of results, including the characteristics of the image retrieval device.

Care should be taken when evaluating the results of a quality control procedure. Results obtained can depend upon the specific output device (e.g. monitor or printer).

If a printer is to be used for quality control procedures, the printer resolution should be equal to or greater than the resolution of the scanned images.

The printer should be capable of accurate reproduction of grey scale or colour in applications where this is relevant.

Where greyscale or colour reproduction is relevant, the accuracy of rendition of grey scale or colour should be evaluated.

Where dimensional accuracy is important, procedures should be documented for checking that dimensional information is reproduced within tolerance. This might involve, for example, checking that the nominal resolution of the scanner is accurate, so that the dimensions in the electronic image can be determined by counting the number of pixels between specific points in the image.

If the scanner operator checks the quality of images during the scanning procedures, a second quality control procedure should be undertaken by personnel other than those responsible for the scanning. This second quality check might involve statistical sampling techniques.

Quality control procedures should be related to the batch process (if used) as defined in 6.4.3, enabling acceptance or rejection of such a batch independently of any other batch.

The results of all quality control checks should be stored in the quality control log (which can be created manually or automatically).

In workflow environments where every electronic document is viewed within a workflow process and activities explicitly check images for quality and reject unacceptable ones, then these activities might be deemed to be a quality control process.

Where the quality control procedures involve sampling of the scanned images and any related data (such as notes), the proportion sampled need not be fixed but can vary from time to time depending on the frequency of problems encountered or the nature of the source material. Where appropriate, statistical sampling techniques should be used to determine the percentage of scanned images to be checked. For further details of sampling techniques, see ISO 2859-1.

It will not normally be practicable to check all processed material and generally only a proportion of the material processed will be checked. For example, at the start of scanning, initially a relatively large sample can be selected (e.g. 20 %), which can be reduced (e.g. to 10 % or even 5 %) as the consistency of meeting the required quality standards can be demonstrated.

Where quality control consists of sampling scanned images, the frequency of sampling should be documented.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

6.4.6.3 Checking scanner performance

Scanner performance checks should be used periodically to monitor the system, to check that it is within agreed tolerances.

Hard copy prints can be made of the scanned images of the test targets and compared with the test targets themselves to determine whether the quality criteria are met, as described in the procedures.

Test targets allow objective assessment and measurement of scanner performance. Regular use can show whether the scanner is performing consistently and in accordance with its specification. The test target given in ISO 12653-3 can be used for this assessment.

The frequency of scanner performance checks should be dependent upon system usage and related to expected deterioration in system performance. This might require recommendations from the system supplier and also experience in the use of the system. Initially, it might be appropriate to scan a test target for every few thousand pages scanned.

If double-sided (duplex) scanners are used, double-sided test targets should preferably be used. Single-sided test targets should only be used with duplex scanners if double-sided test targets cannot be obtained.

Test targets are not representative of the paper documents actually being scanned and are not to be regarded as a substitute for the sample set of documents.

6.4.7 Rescanning

Procedures for rescanning paper documents should be documented. Such rescanning might be required if an original image has been rejected, owing to poor quality or other factors.

Procedures should be implemented to ensure that images resulting from rescanning replace the original image and that batch numbering and audit trail procedures are not compromised.

6.4.8 Image processing

Image processing techniques used to improve the quality of an image should be described in the procedures manual.

Where operator-controlled facilities are available for use, details of which facilities are used for a particular digital document should be documented.

6.5 Data capture

6.5.1 Data creation

Where external data is created and stored on the trusted system, required quality levels should be specified. These quality levels should cover accuracy and completeness of captured data.

Data (for example, for the creation of index or other reference information) can also be captured from existing analogue and/or ESI and entered into a computer in a number of ways, including manually (i.e. direct keyboard entry), automated [e.g. bar code reading, optical mark reading (OMR), optical character recognition (OCR), intelligent character recognition (ICR)], or semi-automated (for example, where data captured automatically, e.g. by OCR, is confirmed by manual re-entry). In each case, the issue is to convey confidence that the correct data have been captured. In practice, it can be difficult, if not impossible, to ensure 100 % accuracy in captured data and the user has to assess the risk associated with the existence of errors.

The specified accuracy levels can vary depending on the application and the importance of each particular data item.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

Procedures should be defined for checking that the accuracy levels are maintained. These procedures will typically be based on random or quasi-random sampling of batches of captured data, with comparison against the source material. Batches that fail to meet the required accuracy levels will generally be reprocessed and the results checked again to ensure that the required accuracy levels are maintained.

Records should be kept of the results of all accuracy checking.

Where data is extracted from ESI, the ESI should be stored and associated with the extracted data.

6.5.2 Conversion and migration

Where data is being received from another system (or part of a system), for example, as part of a storage system migration process, then procedures and processes need to be established, implemented and documented for this process.

Where ESI is converted from the current to a new file format, any potential loss of information (including audit trail information) due to this process should be documented.

6.6 Database considerations

6.6.1 General

Application systems and information are the transactional lifeblood of most organizations. This information is typically managed in databases and is at the centre of the application systems that operationally power the organization on a day-to-day basis. The range of these systems managing information in databases is wide and includes, amongst others, enterprise resource planning (ERP), finance and accounting, human resources, customer relationship management (CRM), etc.

In order for structured information held in databases to be relied upon in the event of disputes, there are many similarities with the trustworthiness aspects of unstructured information. The policy, duty of care, processes and procedures, enabling technology and audit of the trusted system are equally important.

Where information stored in databases is within the scope of the trusted system, the policies, processes, procedures, enabling technology and audit should each specifically reference this information.

In spite of many similarities, there are a number of areas that need to be considered specifically as they are not directly analogous to the trustworthiness issues of unstructured, document-centric, information.

6.6.2 Database systems

6.6.2.1 Extract, transform and load

Extract, transform and load (ETL) refers to a process in database usage, and especially in data warehousing that involves extracting data from outside sources and transforming it to fit operational needs, which can result in significant changes to the information.

Any such change should be able to be explained and justified.

It is important to note that ETL processes can involve considerable complexity and significant operational problems can occur with improperly designed ETL systems. Where ETL has been deployed, all processes should be fully documented, as the source and target databases may have, as a consequence of the ETL process, what appears to be the same information that is not the same in the different databases involved.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

© ISO 2017 – All rights reserved

Where ETL techniques are employed for information stored in structured databases within the scope of the trusted system then:

- changes or loss of information caused by extraction, translation or load should be evaluated and accepted by the organization;
- processes and acceptance criteria should be documented;
- test plans, scripts and results should be retained;
- where audit trails of ETL operations are generated, these should be retained for as long as the information itself.

6.6.2.2 CRUD

A common approach to four basic functions implemented for information in databases is covered by the term "CRUD"; this acronym expands to:

- create;
- read;
- update;
- delete.

There is commonality of the issues surrounding creation, reading and destruction between unstructured and structured information. However, updating is significantly different for structured information in databases from unstructured information.

When unstructured information is updated, a new version is created (see 6.19 on version control). In databases, the update will change the contents of a particular piece of data in the database.

The transaction that resulted in the update to a particular field *in situ* may or may not be retained. This is an area that should be considered and the results of that consideration documented. If the updating transaction and the content before the update are not retained, then it may be necessary that the "before" and "after" contents of the field are able to be re-created in the event of a challenge to trustworthiness. This could be within the audit trail.

The audit trail and/or the definition of the process/procedure should indicate who or what was responsible for the creation, updating, reading or deletion of information in the database. It is worth noting that this responsibility could be a person, a device or an application component/service.

6.6.2.3 ACID

ACID (atomicity, consistency, isolation, durability) are properties that ensure database transactions are processed reliably. Typically, relational database management systems achieve these automatically but it should be noted that a number of NoSQL databases that have been introduced to meet the demands of big data do not include ACID transaction support.

A database system that does not include ACID transaction support might not be updated with every transaction posted to it. This may not be a problem for an organization using such a system.

If the database is not designed based on ACID, then the reliability and trustworthiness of the information content in the database may be questionable.

If the database system deployed is not based on ACID, then the organization should evaluate the impact and formally record evaluations and decisions. It should be noted that suitable application design may meet the ACID transaction support criteria even if the database system does not.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

6.6.3 Database schemas

For a database, the schema defines the tables, fields and relationships of the database itself. This gives context to the data held in these tables and fields enabling it to be information.

A field in a database may contain a number which could be a quantity of an item, a telephone number or a product code. The schema should describe which of these (or others) number actually means. In this respect, the schema can be regarded as metadata that gives context to the field enabling it to be regarded as information rather than simply data.

Sometimes organizations will use a field for a different purpose to that intended and this can be a cause of confusion if not properly considered and documented. In this event, the contents of a field and the schema expectation may be completely different. Such usage is often because the organization does not wish to undertake a costly bespoke modification to a packaged application system. This type of field misuse should be avoided; if it is employed, it should be fully considered, approved and documented.

Another area of concern, especially with packaged application systems, is bespoke extension of the standardized schemas. This will frequently generate customized tables and fields with organization-specific relationships to the standard application system. All such custom schema and application components should be properly considered, justified and documented. This type of customization is frequently the cause of considerable cost and difficulty when the standard application is upgraded to a newer version and can result in compromise to the trustworthiness of the information within the database.

Special care needs to be taken when any schema is modified that the changes are justified and documented and that data migration during the change process is properly tested and results recorded.

When a schema is changed, it is quite common for additional checks to the contents of fields to be applied. However, in practice, the effort to retrospectively apply these additional checks to historic data can lead to a situation where the migrated data is not validated against the new rules but migrated "as is" when the new schema version is introduced. This can lead to situations where old data is in a different format or does not match the validation rules of newer data in the same fields. Such situations need to be able to be explained satisfactorily in the event of a challenge to information trustworthiness.

When a database schema is changed, there are many aspects that should be addressed in order that the schema change is not the cause of unintended compromise to the trustworthiness of database content.

Access to previous schema versions may be required so that, for example, if a database record or field is used as evidence, the database schemas that were in force at the time of its capture and since that time can be described and attested to. If this is not done, there is a risk that the trustworthiness of the information might be successfully challenged.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

6.6.4 Master data management

A challenge facing many organizations is master data management (MDM). MDM aspires to ensure there is a "single version of the truth" across the systems used by an organization as opposed to multiple, inconsistent versions of the same thing held in separate systems.

MDM aims to avoid the need for separate updating of systems by keeping a single master that is used by the different systems and is, as a result, consistent.

Where MDM is deployed, the responsibilities for the master need to be clearly documented.

Where MDM is not, or only partially, deployed, the different versions of the same information should be understood and documented so that a challenge attempting to discredit on the basis of differences between what appears to be the same information can be rebutted.

6.6.5 Transactional vs. updating

There might be a need to be able to show, historically, what the contents of a database were at a specific point in time. In many systems utilizing a database system, there are requirements to be able to show what the information contents of a field were before and after an update or deletion, to avoid or resolve a dispute, while in other situations, this requirement may be superfluous.

The organization should evaluate and record decisions taken in this regard.

When the before and after update information is needed, then this may be achieved by either retaining the before and after update content or by retaining the transaction and being able to deduce the database state preceding the update (this latter procedure may not be feasible for particular updates).

Taking this to the next logical stage, there may be circumstances in which it is necessary to be able to show what the information state of the whole database was at a particular point in time, rather than simply the contents of a particular field or table. This is most likely to be in situations where information from the database is routinely required to be used as evidence.

6.7 Indexing

6.7.1 General

Indexing is a vital part of the process of managing ESI on a trusted system, as it allows access to the relevant ESI. Where indexing information is lost, then the ESI might also be lost.

Indexing can be either automatic (i.e. performed by the system without operator intervention), or manual. If manual indexing is performed, it is important to ensure that the documented procedures be followed.

Some systems allow partial index information to be stored when the ESI is captured. This can then be combined with additional manual index entries at a later time.

Procedures and rules for indexing ESI should be documented.

6.7.2 Manual indexing

Manual indexing involves the visual examination of ESI captured by the trusted system, either during its capture or as part of post-capture processes.

Staff involved in manual indexing should receive specialist training in order to maximize accuracy. Indexing training requirements and procedures should be documented.

6.7.3 Automatic indexing

Automatic indexing can be achieved by, for example, the reading of bar codes or specified data fields, or the use of OCR/ICR techniques. Where automatic indexing is used, procedures to check and amend inaccurate index data should be documented.

6.7.4 Index storage

Index data should be retained for at least as long as the ESI to which it relates is retained.

Some systems require database indexes to be rebuilt periodically, typically to improve database performance. Procedures for rebuilding indexes should be documented.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

6.7.5 Index amendments

Indexing processes can include procedures for the detection of missing ESI. Indexing from displayed ESI may not detect missing material unless the displayed ESI is checked against the original ESI or there is a defined sequence of ESI (for example, by sequential page numbering).

Procedures for the amendment and/or correction of indexing data should be documented. If an index entry is amended, details of index content before and after the change might need to be retained.

Where an index entry relates to deleted or expunged ESI, this status should be stored.

Where, by the amendment or deletion of index entries, deletion or expungement of ESI might be required to comply with legal or regulatory requirements, procedures to be followed should be documented.

6.7.6 Index accuracy

Index data can be inaccurate. While accurate indexing will facilitate the retrieval of ESI, the trustworthiness of that ESI may be demonstrated if its relevance and completeness can be indicated from the accuracy of the relevant index data. Conversely, inaccurate index data can result in the user being unable to retrieve relevant ESI, or retrieving irrelevant ESI.

Index data accuracy criteria can vary depending upon the application. In some cases, the accuracy can be defined as the maximum acceptable number of characters in error per thousand characters captured (or percentage equivalent). In other cases, the accuracy can be defined as the maximum acceptable number of words (or similar cluster of characters, for example, a customer or part number) containing any error (whether of one or more characters).

Criteria for index data accuracy levels should be realistic, given the method used for index data capture, the typical random error rates achieved by data entry personnel and the legibility of the source material. These accuracy levels can vary depending upon the type of ESI being indexed.

Where manual or automatic indexing is undertaken, accuracy levels should be agreed and documented. Procedures for index data accuracy checking should be documented.

6.8 Authenticated output procedures

Output from information management systems, either in the form of paper copies or as ESI on appropriate storage media, might need to be produced for use as evidence. Generally, these copies need to be confirmed as true copies of any related original, in accordance with local requirements, in order to reduce the likelihood of rejection or challenge.

Procedures for the creation of copies of ESI that might be required as evidence should be documented. Such procedures might, for example, require the use of standard system features for copying and written confirmation by an authorized person that the copying process has been conducted correctly. The procedures might specify how such copies are subsequently to be handled. The procedures might refer to audit trail data as a confirmation of the processes that occurred during copying.

Where a paper document is produced as part of the output, the procedures should include the use of an authorized signature or other procedure to confirm the trustworthiness of the copy document.

It is important that the nature and extent of any changes introduced by the retrieval facilities be understood and their relevance assessed. What is acceptable in normal usage might be unacceptable in other circumstances requiring output for use as evidence. For example:

- rendering a coloured image in monochrome might be acceptable in situations where the colour is irrelevant, but in other situations, the colour might be vital, necessitating a different retrieval facility;
- viewing an image at a lower resolution than that used in scanning the original paper document might be acceptable in routine retrievals, but the fine detail which is thereby lost might be important in other situations where, for example, it might have forensic significance;

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

© ISO 2017 – All rights reserved

- where there is not an exact match between the resolution of a scanned image and the retrieval device, the dimensional accuracy of the reproduction can be lost;
- where a stored data file is normally converted to another format for display or printing, information can be lost or presented in a different form, caused by loss of detail or layout differences; these differences might be unacceptable for disclosure and in these cases different retrieval facilities might be required, which do not involve conversion.

If the system facilities used to retrieve, display and/or print ESI do not maintain the layout of the original (e.g. font, pagination), information retrieval characteristics should be agreed upon and documented.

6.9 ESI transmission

6.9.1 Intra-system ESI transfer

6.9.1.1 General

Intra-system ESI transfers are those that take place within the system as defined in 7.2. Intra-system file transfers include:

- local area network transmissions (see 6.9.1.2);
- movement between storage sub-systems under system control, e.g. in a hierarchical storage management system, or between cache and magnetic disk;
- transfer between storage sub-systems under operator control.

In such transfers, the procedures, both electronic and manual, are under the control of the organization. Procedures and processes should be implemented to ensure that the trustworthiness of ESI transferred within the system is not compromised.

ESI transfers from one device to another should be controlled by the appropriate transmission software.

Where additional security measures are required, the use of digital signatures should be considered.

NOTE This subclause is not applicable to the requirement for file migration, where the media type and/or format of the data file might change for technology migration reasons. For further information, see 7.10.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

6.9.1.2 Local area network transmission

In some applications, ESI can be transferred under operator control from one storage device to another using a local area network as defined in 7.2. Local area networks can include connections between remote locations using fixed lines.

Where ESI is transferred using a local area network, procedures and processes should be implemented to ensure that the trustworthiness of transferred ESI is not compromised.

Where ESI is transferred between remote locations using a fixed (e.g. leased) communications line, procedures and processes should be implemented to ensure that the trustworthiness of transferred ESI is not compromised.

6.9.2 External transmission of files

This subclause deals with ESI transmitted between one system and another through external, wide area, communication systems. Such systems are external to the system described in Clause 7. The sending and receiving systems are remote from each other and can be within the same or different organizations. In either case, another party provides the transmission service.

The communication system can involve real-time transmission or deferred (store and forward) transmission such as occurs in e-mail services.

This document is concerned with the trustworthiness of ESI that has been transmitted to another party and with the trustworthiness of ESI received from another party. This document is not directly concerned with the transmission service. By following the recommendations in this document, users can show that a copy of ESI which was transmitted at some previous time to another party has not been altered since that time and that ESI received at some previous time through a transmission from another party has not been altered since the time of receipt.

ESI transfers from one device to another should be controlled by the appropriate transmission software.

Where ESI is copied to another party through a transmission, the original ESI should be retained within the original system for as long as is appropriate. The date and time of any ESI transmission should be stored as part of the audit trail.

Where ESI is received from another party through a transmission, that ESI should be stored within the receiving trusted system. The date and time of any ESI receipt should be stored as part of the audit trail.

Differences between sent and received ESI might be caused by errors in transmission or by deliberate alteration of ESI. There might also be appropriate changes (typically additions) to the metadata of the transmitted ESI. Demonstrating that received and sent ESI contain identical information is no different from demonstrating that any two copies are equivalent. The primary need is to show which ESI is the source and which ESI is the copy, i.e. which ESI existed first. In some instances, this requirement can be met by comparing the times at which the two ESI were stored. If system time clocks are accurate (and bearing in mind differences in time zones), received ESI should have been stored later than that at which the source ESI was transmitted. Thus, the issue becomes one of being able to demonstrate the reliability and accuracy of the timings of the two events.

Hashes, digital signatures, seals and time stamps, for example, can be used to permit confirmation that electronically/digitally signed ESI is exactly the same as was sent and to confirm the identity of the sender. This confirmation of identity might be compromised if the original certificate is no longer valid and maintained by the certifying authority. If the electronic/digital signature certificate is no longer available or expired, the electronic/digital signature will provide information related to whether the ESI has been modified since the time of signing only.

Additional procedures (outside the scope of this document) can be adopted for security or other reasons, e.g. to prevent unauthorized disclosure of the information contained within ESI.

Where it is important to be able to demonstrate that ESI has been delivered, the sender might require that the receiving system transmit back to the sender a confirmation of receipt, which should include the transmission identifier and the date and time of receipt.

If these procedures are followed, then the risk is reduced that ESI has been modified or has been sent from someone other than the identified sender.

The level of security risk being taken during external ESI transfers should be assessed to ensure compliance with the requirements of the information security policy.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

6.10 Information retention

ESI will be required to be retained for legal and/or business purposes for an agreed amount of time (as documented in the retention policy). Procedures should be developed and documented for the retention of ESI until the end of its retention period.

Procedures for the identification of ESI for which fraud has been identified, or for which litigation is envisaged or ongoing, should be documented. Such procedures should include the suspension of disposal policies for this ESI.

Where paper documents are scanned and the information management policy document states that it is general policy to destroy a specific type of paper document, there can be some instances in which an exception applies and the paper document should be retained. It should be noted that,

© ISO 2017 – All rights reserved

where an “original” paper document is retained, access might be required in order to demonstrate the trustworthiness of the electronic “copy” ESI.

Procedures that identify specific paper documents that need to be retained should be documented. Circumstances where this might be required include the following:

- the paper document is of poor quality, so that a legible image cannot be obtained;
- the paper document can be kept to reduce the possibility of it being suggested that the image was deliberately made illegible; this also avoids any risk of rejection of an image on the grounds that it is not a facsimile of the paper document;
- a note can be stored which states that the original paper document was of poor quality and includes details of any visible information that needs to be stored;
- a paper document contains physical amendments or annotations that cannot be identified as such on the scanned image;
- a separate record that physical amendments or annotations were present on the paper document, plus details of what the physical amendments were, can be sufficient;
- fraud has been identified or litigation is envisaged or ongoing;
- the paper document is of high value, such as the signed original of a large contract.

6.11 Information preservation

Procedures for the long-term preservation of ESI should be documented. Such procedures should take into account the required retention periods and the expected life of the trusted systems. Where the retention period exceeds the likely life of the trusted systems, plans for the migration to new systems should be documented (see also 7.10). For further information, see ISO/TR 18492.

6.12 Information destruction

Procedures for the destruction or disposal of ESI at the end of the retention period should be documented.

These procedures should incorporate security precautions appropriate to the sensitivity of the ESI being destroyed.

In the case of capture of analogue documents as ESI, no original documents should be destroyed until the images have been successfully written to storage and appropriate backup procedures have been completed.

6.13 Backup and system recovery

Effective procedures for the backup of ESI should be implemented, with at least two up-to-date copies being created for use in the event of loss or corruption of part or all of the live ESI. It is vital that backup ESI includes all associated information (such as index files, audit trails), so that a complete new system can be built in the event of a total loss of the original system.

The procedures should include the secure remote storage of these backups.

System recovery procedures also need to be documented to demonstrate that such procedures are controlled and tested for reliability.

Issues surrounding the security of backup information might be important in the event of a dispute over trustworthiness. It can be argued that backup media had been compromised and then used to recover from an information loss, thus, affecting the trustworthiness of ESI. In some cases, the availability of backup ESI which has been in secure storage, to be used only in the event of a challenge to the trustworthiness of the live ESI, can be used to enable the demonstration of trustworthiness of the ESI.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

Facilities on the system should allow for the backup and verification of all ESI and associated information, including audit trails, at regular intervals.

There should be information kept in the system audit trail of all backup activity, which should include details of any problems incurred during the procedure.

If the file structure of the ESI held on a backup is different to that of the original, the structure of the backup ESI should be detailed in the systems description manual.

The audit trail should detail all ESI recovery activities and include a description of any problems experienced during the recovery procedures.

Procedures for checking that ESI trustworthiness has not been compromised after a restore should be documented. Where backup ESI is used to recover from a system failure, procedures should be documented to ensure that ESI trustworthiness has not been compromised.

Media used for backups do not necessarily provide permanent storage conditions. Media suppliers usually provide information regarding recommended testing frequency. Alternatively, if such specific information is not available, general recommendations can often be found in national or International Standards.

Testing media on the same hardware each time is no guarantee that the media can be read on other devices, even from the same supplier and of the same model type. Backups are of no value if the only hardware that can read them is lost.

Backup media should be tested at regular intervals, using a variety of hardware to read the media.

6.14 System maintenance

6.14.1 General

The trusted system should be maintained and corrective maintenance carried out only by qualified personnel to ensure that its performance does not deteriorate to such an extent that the trustworthiness of the ESI managed by the trusted system is affected.

For example, it is of specific importance in a paper document scanning system that it be maintained in accordance with the manufacturer's specifications, in order that image quality is maintained.

Preventative maintenance should be carried out regularly, in accordance with the supplier's recommendations. Preventative maintenance may involve the maintenance of the patching history of the trusted system.

Procedures used for preventative maintenance should be documented.

These procedures can be performed by system operators or by specialized service personnel.

A maintenance log should be kept, stating the preventative and corrective maintenance procedures completed.

Procedures to control the use of system maintenance hardware and/or software that can bypass system access controls should be documented. Access to such tools and facilities should be strictly controlled and monitored.

Information regarding system downtime and details of action taken should be stored in the maintenance log.

6.14.2 Scanning systems

Where paper document scanning is implemented, procedures described under the quality control section should be used to check that a scanning system continues to produce the output quality required of the system after the maintenance procedures have been completed.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

© ISO 2017 – All rights reserved

These test results will serve to confirm, at any later date, that any poor quality images were not due to malfunction of the system. If there is any deterioration in the output quality, appropriate corrective maintenance is necessary.

6.15 Security and protection

6.15.1 Security procedures

Security guidelines that are applicable to the organization and application concerned should be implemented. Such guidelines, for example, might exist in company policies or practice, sector-specific guidance (e.g. financial, medical), national or International Standards, or as legal requirements.

In the absence of internal guidelines, published information can provide comprehensive security guidelines that are designed to meet the organization's needs. They might provide an adequate basis for the creation of guidelines that would meet the organization's requirements. Some organizations might consider the adoption of externally accredited security schemes as additional confirmation of compliance with their security policy.

Procedures implemented in accordance with the organization's information security policy should be documented.

To control access to the various levels of the system (e.g. manager, data input and retrieval), a secure access control system should be implemented.

The accommodation and operating environment for trusted systems and for the storage, labelling, handling, transportation and maintenance of storage media should be in accordance with suppliers' recommendations and/or relevant national or International Standards.

The central part of the system (including servers and storage devices) should be installed in secure areas (as defined in the organization's security procedures), with documented restricted access.

6.15.2 Encryption keys

Encryption techniques can be used to protect the trustworthiness of ESI. ESI can be encrypted so that the information it contains cannot be retrieved without the use of a decryption key. Encryption is a complex topic and one that is constantly changing. Readers should refer to authoritative publications on this topic for detailed information.

The use of encryption for long-term storage can be problematic, should the keys and/or certificates become unavailable for any reason.

Where encryption is used, keys should be kept securely and should not be available except to those authorized as responsible for activities requiring access to the keys.

Procedures should be implemented for encryption key allocation and management and for certificate management.

Where encryption is used and additional benefits can be obtained from third-party key management/recovery and key escrow services, their use should be considered.

The person who originally was responsible for managing the keys and certificates securely within the organization might no longer be employed, so procedures are required to ensure their continued availability.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

© ISO 2017 – All rights reserved

6.16 Use of contracted services

6.16.1 General

Specialist service providers are often used for, for example, paper document scanning, indexing, data conversion, storage and other services.

a) A contract should be agreed upon with the service provider that details the services that are to be used.

b) If the contract does not require that the contractor comply with all relevant recommendations of this document, the user's inspection procedures on services provided should be such that no assumptions are made regarding the completeness, quality and accuracy of the services.

The procedures and recommendations in this subclause cover any type of service, including those provided on a facilities management basis and is intended to ensure:

— that where work is carried out by a service provider, the procedures for the demonstration of trustworthiness of the resulting ESI will be the same as if the work had been done wholly within the client's organization;

— that the client can demonstrate compliance, many years after the event, even if the service provider has ceased to trade.

Where work is undertaken off-site, details of the procedures used in the transfer of information and/or media from the client to the service provider and from the service provider to the client should be documented.

If the service provider uses procedures which comply with the policy document, the client should hold a copy of, or have access to when required, the service provider's compliance documentation.

6.16.2 Procedural considerations

In ideal circumstances, where the service provider can demonstrate the implementation of procedures which comply with the information management policy document, the contract need only confirm this situation and contain agreed procedures for checking compliance.

Where the service provider operates in compliance with agreed procedures, the contract should include a statement detailing the extent to which the procedures are implemented and audited.

The following list defines procedures and processes that may need to be reviewed and included within the contract as appropriate.

— The client should check that the service provider can produce output to agreed acceptable quality standards.

— The client should check that the service provider can process a sample of information to produce output on the proposed media and in the proposed format and which can be successfully loaded on the client's target system. This sample should be retained.

— The client should check that the service provider can supply a copy of the audit trails of the processing undertaken in a readable form.

— Where indexing services are provided, the client should check with the service provider that the proposed indexing data accuracy requirements are acceptable and documented.

— The client should check that the proposed location of the work is acceptable and meets security criteria appropriate to the client's needs.

— The client should check that the proposed procedures and processes involve no greater risk of damage to the client's information than the client's procedures.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

- The client should check that, where the information to be processed is unique or particularly valuable, effective fire detection and prevention systems are implemented at the proposed production location.
- The client should check that, where security of the information to be processed is important, the service provider should vouch for the trustworthiness of the intended operational staff. It is an advantage if all employees of the organization sign a confidentiality agreement as part of their conditions of employment.
- Where paper documents are sent for scanning, the service provider and client should make arrangements for the documents to be accessible to the client while they are away from the client's premises.

6.16.3 Transportation of paper documents

Where paper documents are physically moved from the client's to the service provider's premises, opportunities exist for their loss or damage. Procedures need to be agreed upon to ensure that this risk is acceptable. Each shipment of documents to or from the client and the service provider should be accompanied by a control document stating the identity and number of items included.

All documents being shipped should be adequately packed to avoid risk of damage in transit.

The recipient should promptly check received documents against the despatch document and advise the sender of discrepancies as soon as is practically possible.

Transportation services can be provided by the user's own organization, by a third party or by an independent courier.

Third parties providing transportation services should be organizations demonstrably meeting the quality and reliability criteria of the client.

Notes should be taken of the date and time at which the documents were handed over to the transportation service and the date and time at which it was received by the service provider and signed by the person handing over and receiving the documents. The same process should be implemented on receipt of returned documents.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

6.16.4 Use of trusted third party

A secure means for detecting any tampering with ESI, or for verifying the contents of particular ESI, is to store a copy of the ESI or its hash value with a trusted third party.

If such an approach is taken, an authenticated copy of the ESI should be made and delivered either physically or electronically to the trusted third party, using secure means.

The trusted third party should follow the relevant procedures for the management of ESI as recommended by this document and should be able and prepared to demonstrate, in the same manner as the owner, the effectiveness and security of its services.

NOTE Security requirements for trusted third parties are frequently more stringent than those for the organization whose ESI they are managing.

Where digital signatures are used for authentication, instead of storing digital signatures in its own system, the organization can transmit the digital signature associated with particular information to the trusted third party. The third party will store the digital signature in secure conditions, such that it can be retrieved later.

6.17 Workflow

Some trusted systems incorporate a workflow capability. Such systems provide the procedural automation of business processes, by the management of the sequence of work activities and the invocation of appropriate human and system resources associated with the activity step.

Where workflow systems are implemented, operational details (such as flow diagrams), process definition classifications and process definitions should be documented.

Process definition lifecycles include:

- definition;
- development;
- implementation;
- withdrawal;
- modification.

All ESI (databases, audit trails, etc.) held on the workflow system should be reviewed for retention requirements and, where applicable, stored in compliance with the information management policy document.

Where changes to the workflow system are implemented, change control procedures should be implemented to ensure that ESI is not lost during the procedure.

Where an ad hoc workflow is implemented (i.e. one in which the rules can be modified or created during the operation of the process), a full audit trail of the process should be kept together with the identification of personnel who performed the changes to the standard workflow procedures.

6.18 Date and time stamps

Procedures for the regular checking of system clocks for accuracy concerning date and time should be documented. Any errors should be corrected and any actions taken documented.

If the clocks are changed on a seasonal basis, e.g. summer time, then the procedures to be followed should be documented.

Only authorized personnel should be able to change system clocks.

Where there is a particular need to demonstrate the accuracy of date and time stamps, the use of trusted third-party services for this can be considered. Where trusted time is used, procedures for demonstrating the trustworthiness of a time stamp and its binding to particular ESI should be documented.

6.19 Version control

6.19.1 Information

In some applications, ESI might be subject to change. Several different versions of ESI might be developed over a period of time; in this case, iterations should be allocated version numbers. It is important in such applications to maintain each version as separate ESI and also to maintain the link between the versions.

Where changes to stored ESI are allowed, the procedures for authorizing and implementing such changes should be documented.

Documentation regarding any requirement to retain previous versions of such ESI should be available.

6.19.2 Documentation

A version control system should be implemented to ensure that the relevant version of any compliance document can be identified for any time in the life of managed ESI. A version control procedure should be established for all documentation.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

© ISO 2017 – All rights reserved

Superseded versions should be kept for at least the same length of time as that for which relevant ESI is maintained.

Records of this maintenance are required so that the policies and procedures which were in force at the time of its capture, and since that time, can be described and attested to. If this is not available, there is a risk that the trustworthiness of the ESI might be successfully compromised. For example, if it is not possible to be certain of the scanning procedures used to capture the image of a paper document several years old and the storage procedures followed in the years since its capture, then it might be difficult or impossible to refute a challenge concerning the trustworthiness of the ESI.

6.19.3 Procedures and processes

All changes to procedures and/or processes should be implemented in accordance with an approved change control procedure.

6.20 Maintenance of documentation

Compliance with the information management policy document requires the availability and use of specified documentation. Procedures for the maintenance of this documentation should be included in the procedures manual. Maintenance procedures should include the keeping of records of this maintenance.

Maintenance is required because, over time, requirements will evolve and technologies and legislation will change. In some cases, it will suffice for maintenance efforts to be driven by recognition of changes on an ad hoc basis. Additionally, typically for more important ESI, a routine regular review will be appropriate.

Procedures for ensuring that documentation is kept up to date should be documented.

This documentation should be subject to records management disciplines which are at least as good as those applied to the organization’s other business records.

In particular, whenever one of these documentation items is revised, a copy of that item prior to the change should be kept at least as long as the ESI to which it relates.

The storage of this documentation should allow for appropriate authorized parties (e.g. auditors) to identify and retrieve all the documentation in force on any required date.

Documentation can be stored electronically in the trusted system, subject to the same controls as included in this document, as paper or microform in secure locations, or as any combination of these.

The policy adopted for the storage of compliance documentation should be documented in the policy document.

In most cases, it will be desirable for changes to be documented in a way that allows an interested party to track the changes between versions. This can be implemented by recording a simple change history for each part of the documentation.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

7 Enabling technologies

7.1 General

This subclause deals with technology-related topics that are relevant to this document, including the following:

- system description manual (see 7.2);
- storage media and sub-system considerations (see 7.3);
- access levels (see 7.4);

- system integrity checks (see 7.5);
- image processing (see 7.6);
- compression techniques (see 7.7);
- form overlays and form removal (see 7.8);
- environmental considerations (see 7.9);
- migration (see 7.10);
- information deletion and/or expungement (see 7.11).

Where appropriate, the guidance given in ISO/TR 22957 should be taken into consideration when the requirements for the trusted system are being analysed, selected and/or implemented.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

7.2 System description manual

A description of hardware, software and network elements that comprise the trusted system and how they interact should be included in the system description manual.

Details of trusted system configurations should be documented.

Details of all changes to the trusted system should be documented. Such documentation should include details of any processes implemented to effect the change.

The system description manual should be structured so that details of the trusted system at any time during the period of its use can be readily accessed. This can be achieved by creating a new version of the manual every time there is a change, such that it is possible to gain access to a clear description of the trusted system as it was at a particular time in the past.

For information management systems already in operation, ESI managed by the trusted system prior to the achievement of compliance with the information management policy document cannot be considered as meeting its provisions unless the controls and procedures described in this policy document have been in place from the time of acquiring that ESI.

The user should assess whether the elements of the trusted system conform to the requirements of relevant national and/or International Standards. This enables system auditors to check the performance and reliability of the trusted system against these standards.

7.3 Storage media and sub-system considerations

The risk of stored ESI being modified inadvertently or maliciously varies with the type of storage sub-system and medium. The ability to detect any such modifications also varies. For example, where write-once media is used, it is not normally possible to modify ESI once stored, as any such modification would have the effect of destroying at least some information, resulting in ESI being corrupted, if not made totally irretrievable. Conversely, in the case of trusted systems which use online storage (including the use of cloud storage systems), unauthorized modification, which is typically managed by access control, can never be totally guaranteed.

ESI stored on magnetic disc and other random access rewritable media can, in principle, be modified. With such media, the risk of modification is less to do with the medium itself than with the controls that are implemented by the storage sub-system and by the access software. The ability to alter ESI requires read-write access and well-designed trusted systems have controls to prevent unauthorized read-write access. Users with read-only access are unable to modify the ESI. This alone is unsatisfactory unless the trusted system also maintains a secure record of all read-write accesses. In a trusted system where there are very frequent ESI modifications, there might be a substantial overhead to record these modifications, but if a record is not kept, it might prove impossible to detect any unauthorized alterations by a skilled hacker or by anyone with the appropriate access privilege.

© ISO 2017 – All rights reserved

In the case of rewritable serial media, such as magnetic tape, unauthorized tampering can be more difficult than with random access media, since if the ESI that is modified is not usually the last ESI stored on the medium, then all following ESI needs to be copied and rewritten. Once the medium is off-line, it could be tampered with more easily if an attacker were able to gain access to it. The issue of physical security of the off-line medium and access control while it is online is important.

The point in the application processes at which ESI is requested by the software to write to storage should be documented.

Storage media and associated sub-systems should be chosen such that inappropriate additions, alterations and/or deletions without detection are prevented. Detection procedures can involve use of electronic/digital signatures and/or copies that are stored in different locations, possibly involving trusted third parties.

In systems that do not include facilities that in the course of normal operations would automatically detect unauthorized alteration to or removal of ESI, users should conduct random checks to verify that ESI which has been frozen has not been altered or removed.

Where write-once media is used, consideration should be given to the retention period of the ESI being managed. Where practical, ESI with differing retention periods should not be stored on the same physical piece of medium.

7.4 Access levels

Detail of all levels of access available in the system and procedures for their use should be documented. These levels are usually available as follows:

- system manager;
- system administrator;
- system maintenance;
- authors or originators;
- information storage and indexing;
- information retrieval.

Only staff with the relevant access rights should be permitted to enter or amend ESI.

System access rights should be granted only after the member of staff has successfully proved his or her competence.

7.5 System integrity checks

7.5.1 General

Facilities should be provided within the system to ensure that the trustworthiness of ESI is preserved throughout the system, including during its transfer to and from the storage medium.

A suitable approach is to utilize a checksum or hash value calculated immediately after the ESI has been captured. This technique ensures that any errors in ESI transfer between sub-systems can be detected automatically and with certainty. Such a method on its own does not cover the possibility of malicious manipulation of the ESI between the time of capture and the time of committal to the storage media. Such manipulation could be accompanied by the calculation of a new checksum or hash value if the checksum or the hash value algorithm were known or deprecated. To deal with this eventuality, other procedures are required. A simple method is to write each checksum or hash value to the audit trail after calculation and protect the audit trail from manipulation.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

To protect the ESI from malicious software, appropriate protection software should be installed and kept up to date.

Where appropriate, hardware to protect the system from power failure should be installed.

7.5.2 Digital and electronic signatures (including biometric signatures)

Digital and electronic signatures offer the possibility of demonstrating that retrieved ESI is exactly what was acquired. The implementation of these signature systems usually requires the cooperation of both parties. Signatures are either created with signature digitizing devices (electronic) or using a key (digital) and are associated with the ESI. In some cases, the retriever might use the signature to verify the identity of the original signatory and, with some signature systems, the trustworthiness of the ESI. This applies to storage, workflow or transmission, whether real-time or store-and-forward transmission systems are used. Signatures should be used in applications where it is important to be able to confirm the trustworthiness of received ESI and potentially the identity of the sender. Signatures should be stored securely. Access to signature files, keys and algorithms should be allowed only to authorized personnel.

Digital and electronic signatures used to demonstrate the non-alterability of ESI should include a checksum or hash value embedded in the ESI and/or stored in a secure system bound to the original ESI.

Processes used for the issue, maintenance and/or creation of digital and electronic signatures should be documented. These processes should include mechanisms for verifying the true identity of the person prior to that individual being enrolled as a signatory.

If a query is raised about the trustworthiness of ESI, signatures can be used as evidence in demonstrating that any ESI received by transmission contains the same information as the original ESI. Processes to be implemented where a query is raised about the trustworthiness of ESI containing a digital signature should be documented.

7.6 Image processing

Where scanning processes have been used, post-scanning processes can be performed to achieve optimum image quality, or to improve recognition rates for an automated data capture process. Where post-scanning processes are performed, the effect on the image of each of these processes should be individually documented.

The term post-scanning processes is used to describe various image enhancement techniques using hardware and/or software that can singularly or independently have an effect on the presentation of image output and the size of the stored ESI. They can be installed either on a scanner workstation or on a network server.

The more common techniques include:

- de-skew;
- de-speckle/background clean-up;
- black border removal;
- form removal (see also 7.8).

Image processing facilities should be used with care. For example, the de-speckle process might remove decimal points, thus, altering the value of numbers.

Any processing performed on the digitized image should not affect the trustworthiness of the image as a true facsimile of the original. To check that any image processing does not affect the trustworthiness of the scanned images, a sample set of paper documents should be scanned with the image processing active and prints of these images compared with the originals.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017

Where image processing techniques are used, consideration should be given to storing images of the sample set of paper documents with and without image processing.

The effect of processing performed on a grey scale image prior to conversion to a black-and-white image should be checked for acceptability.

Speckle removal should only be used with particular care and its use should be documented. Speckle removal results in the elimination of single pixels or small groups of pixels from an electronic image, resulting in a subjectively cleaner image, but it cannot be relied upon just to remove noise from the image. With some kinds of paper document, there is a high risk that information might be removed, e.g. parts of already broken characters, punctuation marks or parts of fine detail in drawings.

If speckle removal is used routinely on images, then without explicit information on the identity of images to which it has been applied, it can be assumed subsequently that all images have had speckle removal applied. This could affect the ability to demonstrate the trustworthiness of these images, if any doubt were raised about the completeness of the images.

The use of speckle removal can be documented in the operator log, or elsewhere in the audit trail, or by using additional data associated with the relevant image.

Where it is important that there should be no loss of information in the scanned image, other than that due to the scanning resolution, there should be no image processing subsequent to the initial creation of the image file.

Where image processing techniques might affect the trustworthiness of a stored image, consideration should be given to also storing the original (e.g. unprocessed) image.

7.7 Compression techniques

The use of electronic compression techniques should be in accordance with the information management policy document. Such techniques can be applied to ESI prior to, or during storage, to reduce the size of the ESI and/or to improve system performance.

The type of compression used is usually application dependent, though some systems can have built-in compression that the user has no alternative but to use. For further information on compression methods, see ISO/TR 12033.

Compression can use various mathematical approaches, but all can be classified into two classes, namely lossy or lossless.

The compression techniques used and their lossless or lossy attribute should be documented. The documentation should be quantitative and include the algorithm used to compute the extent of loss. This information can be stored as part of the ESI or its related information, or using a separate log.

NOTE For example, in the case of image files stored in TIFF (and some other) format, the compression method is automatically stored within the image file.

Lossy compression techniques should be used with care. By definition, lossy techniques lead to irreversible data loss, even though in some instances, this loss is not visually apparent. Thus, decompressed ESI will not be identical to the original ESI. This might make the demonstration of trustworthiness of ESI more difficult. For example, on an image file, parts of text or drawings might be removed, being replaced by artificially generated information. Thus, there might be risk in using lossy compression on files primarily containing text (including handwriting) or line drawings.

Lossy compression can be suitable for photographic or other continuous-tone material, grey scale or coloured documents where it can be shown that there is no significant loss of information in the scanned image.

If lossy compression is used, a sample set of decompressed ESI should be compared with the originals to check that there is no significant loss of information.

STANDARDSISO.COM : Click to view the full PDF of ISO/TR 15801:2017