TECHNICAL REPORT

ISO/TR 15801

Second edition
2009-10-15

Document management — Information stored electronically — Recommendations for trustworthiness and reliability

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

Reference number
ISO/TR 15801:2009(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

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

This second edition cancels and replaces the first edition (ISO/TR 15801:2004) which has been technically revised.

Introduction

This Technical Report 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.

Information, in the form of digital objects, originates from many sources. This Technical Report covers digital objects 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.

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

This Technical Report describes means by which it can be demonstrated, at any time, that the contents of a specific electronic object created or existing within a computer system have 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 system can be reliably reproduced in a consistent manner and accurately reflects what was originally stored without any material modification.

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

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

Readers are advised to use this Technical Report in conjunction with other local sources, particularly with relevance to governmental and legal requirements in their respective jurisdictions.

Document management — Information stored electronically — Recommendations for trustworthiness and reliability

1 Scope

This Technical Report describes the implementation and operation of document management systems that can be considered to store electronic information in a trustworthy and reliable manner.

This Technical Report is for use by any organization that uses a document management system to store authentic, reliable and usable/readable electronic information over time. Such systems incorporate policies, procedures, technology and audit requirements that ensure that the integrity of the electronic information is maintained during storage.

This Technical Report does not cover processes used to evaluate whether information can be considered to be authentic prior to it being stored or imported into the system. However, it can be used to demonstrate that, once the information is stored, output from the system will be a true and accurate reproduction of the original.

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

2 Terms and definitions

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

2.1
information type
groups of related documents

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

EXAMPLES Invoices, financial documents, data sheets, correspondence.

2.2
trusted system
⟨document management⟩ system used to store electronic information in an accurate, reliable and usable/readable manner, ensuring integrity over time

3 Document management policy

3.1 General

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

Information, like any other asset, 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 information. Additionally, this clause provides guidance to organizations with respect to the level of documentation required to enable an organization to clearly establish how the information contained in a trusted document management system is reliable, accurate and trustworthy. Availability of this documentation can also be used to demonstrate that document management is part of normal business procedures.

Where a system stores information that can be used as evidence in any legal or business process, one's legal advisors should be consulted (see 4.4) to ensure that one complies with relevant legal or regulatory requirements. As legal and regulatory requirements vary from country to country (and sometimes within a country), the legal advice one obtains should cover all relevant jurisdictions.

3.2 Document Management Policy Document

3.2.1 Contents

A Document Management Policy Document (the Policy Document) should be produced, documenting the organization's policy on document management and storage, as applicable to the trusted document management system.

The Policy Document should contain sections which:

— specify what information is covered (see 3.2.2);

— state policy regarding storage media (see 3.2.3);

— state policy regarding electronic object file formats and version control (see 3.2.4);

— state policy regarding relevant document management standards (see 3.2.5);

— define retention and destruction policies (see 3.2.6);

— define responsibilities for document management functions (see 3.2.7);

— define responsibilities for monitoring compliance with this policy (see 3.2.8).

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

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

3.2.2 Information covered

In order to define the organization's document 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. The Policy Document should include, as an information type, all documents produced in compliance with the Policy.

3.2.3 Storage media

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

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

The media type on which each information type (see 3.2.2) can be stored should be specified.

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

The policy for the management of copies of electronic objects should be detailed in the Policy Document.

3.2.4 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 information stored on a computer system requires software for retrieval and display. This software is subject to change, either by the implementation of new releases, or by changes to operating systems and/or hardware. By implementing a policy of approved 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 stored information.

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

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

For additional information on this, see 5.5.2, 5.10, 6.10 and 7.2.3.

3.2.5 Standards related to document management

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

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

3.2.6 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 information.

3.2.7 Document 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.

3.2.8 Compliance with policy

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

4 Duty of care

4.1 General

4.1.1 Trusted system

A trusted document management system is one that ensures that all electronically stored information can be considered to be a true and accurate copy of the original information, regardless of the original format. Trusted document management systems need to include the following as a minimum:

— the creation of at least one copy of the stored information on to media that protects the stored information 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 from the other copy of the stored information;

— the utilization of hardware and storage media that protect the stored information from modification, inappropriate additions or deletion throughout its approved lifecycle (see also 6.3);

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

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

4.1.2 Controls

It is essential that the organization be aware of the importance of designing and maintaining all aspects of the trusted document management 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 electronic information at all levels;

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

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

— implement an Information Security Policy.

4.1.3 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 records (in this respect separation of roles is particularly important in systems where there is risk of fraud or other malicious action).

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

— input reconciliation (see 5.4.3);

— quality control (see 5.4.6);

— data entry (see 5.6);

— information deletion (see 5.11);

— information security (see 4.2).

It is also important to ensure that the physical and managerial segregations that exist around a 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.

4.2 Information security management

4.2.1 Information Security Policy

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

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

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

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

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

The organization should adopt an Information Security Policy, covering all elements of the trusted document management system.

Where the organization has an Information Security Policy for other systems, then the use of the trusted document management system should be incorporated within its scope.

The Information Security Policy Document should contain, as a minimum:

— scope of policy;

— statement of management objectives in respect of security;

— specific policy statements;

— requirements for different information classification categories;

— definition and allocation of information security responsibilities;

— policy for dealing with breaches of security;

— 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 information, in compliance with its Information Security Policy Document.

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

4.2.2 Risk assessment

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

The organization 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).

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

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 cost 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.

4.2.3 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.

4.3 Business continuity planning

From time to time, problems arise with trusted document management 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 integrity of information is not compromised during these operations, an agreed and approved Business Continuity Plan (sometimes known as a Disaster Recovery Plan) can 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 integrity of stored information is not compromised during their implementation.

4.4 Consultations

The implications of using trusted document management 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 authenticity, reliability and integrity of stored information prior to implementing the Document 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 Document Management Policy Document.

These consultations can include the following topics:

— legal issues;

— 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 document management system.

5 Procedures and processes

5.1 General

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

5.2 Procedures Manual

5.2.1 Documentation

The organization should maintain a Procedures Manual for each trusted document management system.

Where, in this section, documentation is required, this documentation can either be included in the Procedures Manual, or referenced by it. This manual can 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.

5.2.2 Content

The Procedures Manual should include or reference procedures for the operation of the trusted document management system and should include the following:

— information capture (see 5.3);

— document image capture (see 5.4);

— data capture (see 5.5);

— indexing (see 5.6);

— authenticated output procedures (see 5.7);

— file transmission (see 5.8);

— document retention (see 5.9);

— information preservation (see 5.10);

— information destruction (see 5.11);

— backup and system recovery (see 5.12);

— system maintenance (see 5.13);

— security and protection (see 5.14);

— use of contracted services (see 5.15);

— workflow (see 5.16);

— date and time stamps (see 5.17);

— version control (see 5.18);

— maintenance of documentation (see 5.19).

For convenience, the Procedures Manual can be maintained as a number of separate physical documents, relating to different document management areas.

Where the organization has multiple trusted document management systems, the documentation can comprise a single Procedures Manual or multiple Procedures Manuals.

5.2.3 Compliance with procedures

In order to be able to comply with the procedures detailed in the Procedures Manual, staff 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 who operate the system adhere to requirements.

5.2.4 Updating and reviews

It is important to ensure that the procedures implemented at any time during the storage life of any specific piece of information 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.

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.

5.3 Information capture

5.3.1 General

Where the trusted document management system is used for storing electronic objects, the procedures involved in the capture of those objects should be documented.

These procedures can include:

— electronic object capture;

— document preparation;

— document batching;

— photocopying;

— scanning;

— image quality control.

Documents can include paper documents or microform documents.

Subclause 5.4 contains further details on the procedures relevant to document scanning.

5.3.2 Information loss

Where electronic objects are stored in a trusted document management system, potentially there is the possibility of loss of some of the information. For example, when scanning a paper document, resolution might be such that small characters are illegible on the digital image; or, where a digital document is converted from one format to another, some metadata can be lost.

Where storage media is changed, physical evidence (such as fingerprints on paper documents or CD media) might not be reproduced within the electronic object. 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 the information is captured and/or retained.

5.3.3 Creation and importing

Electronic information can be created within a trusted document management system, or imported into it. The authenticity of the documents at the time they are created or imported is of critical importance, as the trusted document management system will consistently reproduce whatever information has been stored.

Electronic information can be stored in two forms, either in image or data format. In either form, they can be imported into the trusted document management system in a variety of formats.

Image formats are typically obtained from:

— paper documents (originals, photocopies, faxes);

— automatic facsimile entry (via a fax server);

— capturing screen shots where multiple pieces of information are being displayed simultaneously (also referred to as compound transient documents);

— microfilm and microfiche.

Image formats are typically bit maps of an original analog document. Image formats can also be obtained from digital documents. Details of procedures for capturing analog documents in image format are discussed in 5.4.

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.;

— CAD drawings;

— e-mail messages;

— Electronic Data Interchange (EDI) files;

— instant messages;

— XML messages;

— screen shots (for example, for transient documents).

In all cases, the information contained in the data can be accessed through the use of an appropriate software application. Details of procedures for capturing analog documents in data format are discussed in 5.5.

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

Where information to be stored in the trusted document management system originates from outside the boundaries of control of the organization employing the trusted document management system, there might be little or no control over, or knowledge of, the procedures or processes involved in the production or authorization of that information. In these circumstances, the organization will need to take care that the information 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 information in question.

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

5.3.4 Metadata

When digital and/or analog documents are 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 digital and/or analog documents have the correct interpretation placed on them.

The content of metadata information 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 information to which it pertains. The use of an appropriate metadata schema should be considered.

5.4 Document image capture

5.4.1 General

This subclause includes recommendations relating to the procedures relevant to the creation of digital images from analog documents. Recommendations in this subclause are for users whose trusted document management systems include the capture and storage of analog documents in digital form by the use of scanners. These recommendations cover procedures for:

— preparation of documents;

— document batching;

— photocopying;

— scanning;

— image processing.

5.4.2 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.

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 to 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.

5.4.3 Document batching

Wherever possible, 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.

5.4.4 Photocopying

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

— 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.

5.4.5 Scanning processes

Details of procedures used in analog 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; 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 misfeeds, 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 digital document to be uniquely identified, in such a way that its identity cannot be changed or removed, except as permitted as described in 6.11.

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

5.4.6 Quality control

5.4.6.1 Sample set

Procedures are required which reduce the risk of scanned images being of unsatisfactory quality. It will be easier to demonstrate authenticity 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.

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.

5.4.6.2 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 grey scale 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 digital 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 5.4.3, 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 digital 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, 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.

5.4.6.3 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 12653-2 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.

5.4.7 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.

5.4.8 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.

5.5 Data capture

5.5.1 New data

Data (for example for the creation of index or other reference information) can be captured from existing analog and/or digital documents 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), OCR/ICR], or semi-automated (e.g. 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.

Where external data are captured for entry into the system, required quality levels should be specified. These quality levels should cover accuracy and completeness of captured data.

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

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 an electronic document, the original document should be stored and associated with the extracted data.

5.5.2 Conversion and migration

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

Where information 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.

5.6 Indexing

5.6.1 General

Indexing is a vital part of the process of storing information on electronic media, as it allows access to the relevant information. Where indexing information is lost, then the stored information can 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 information is captured. This can then be combined with additional manual index entries at a later time.

Procedures and rules for indexing stored information should be documented.

5.6.2 Manual indexing

Manual indexing involves the visual examination of information being captured by the system, either prior to 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.

5.6.3 Automatic indexing

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

5.6.4 Index storage

Index data should be retained for at least as long as the information to which they relate is retained.

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

5.6.5 Index amendments

Indexing processes can include procedures for the detection of missing information. Indexing from displayed information will not detect missing material unless the displayed information is checked against the originals or there is a defined sequence of information (for example by sequential 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 information, this status should be stored.

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

5.6.6 Index accuracy

Index data for scanned images can be inaccurate. While accurate indexing will facilitate the retrieval of stored information, the authenticity of that information can 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 information, or retrieving irrelevant information.

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 information 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.

5.7 Authenticated output procedures

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

Procedures for the creation of copies of stored information that might be required as documentary 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 accuracy 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;

— 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 stored information do not maintain the layout of the original (e.g. font, pagination), information retrieval characteristics should be agreed upon and documented.

5.8 File transmission

5.8.1 Intra-system data file transfer

5.8.1.1 General

Intra-system file transfers are those that take place within the system as defined in 6.2. Intra-system file transfers include:

— local area network transmissions;

— 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 integrity of files transferred within the system is not compromised.

File transfers from one device to another should be controlled by the application 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. See 6.10.

5.8.1.2 Local area network transmission

In some applications, files can be transferred under operator control from one storage device to another using a local area network as defined in 6.2. Local area networks can include connections between remote locations using fixed lines.

Where files are transferred via a local area network, procedures and processes should be implemented to ensure that the integrity of transferred files is not compromised.

Where files are transferred between remote locations via fixed (e.g. leased) communications line, procedures and processes should be implemented to ensure that the integrity of transferred files is not compromised.

5.8.2 External transmission of files

This subclause deals with files transmitted between one system and another via external, wide area, communication systems. Such systems are external to the system described in Clause 6. 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 Technical Report is concerned with the integrity of electronic objects that have been transmitted to another party, and with the integrity of electronic objects received from another party. This Technical Report is not directly concerned with the transmission service. By following the recommendations in this Technical Report, users can show that a copy of an electronic object which was transmitted at some previous time to

another party has not been altered since that time, and that a file received at some previous time via a transmission from another party has not been altered since the time of receipt.

File transfers from one device to another should be controlled by the application software.

Where a file is copied to another party via a transmission, the original file should be stored within the system.

The date and time of any file transmission should be stored as part of the audit trail.

Where a file is received from another party via a transmission, that file should be stored within the system.

The date and time of any file receipt should be stored as part of the audit trail.

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

Electronic/digital signatures, for example, can be used to permit confirmation that an electronically/digitally signed document 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 document has been modified since the time of signing only.

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

Where it is important to be able to demonstrate that a file 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 a file has been modified, or has been sent from someone other than the identified sender.

The level of security risk being taken during an external file transfer should be assessed, to ensure compliance with the requirements of the Information Security Policy.

5.9 Document retention

Where paper documents are scanned, and the Document 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, where an “original” paper document is retained, access might be required in order to demonstrate the authenticity of the electronic “copy”.

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.

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

5.10 Information preservation

Procedures for the long term preservation of information should be documented. Such procedures should take into account the required retention periods and the expected life of the storage systems. Where the retention period exceeds the likely life of the storage systems, plans for the migration to new systems should be documented (see also 6.10). For further information, see ISO/TR 18492.

5.11 Information destruction

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

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

No paper documents should be destroyed until the images have been successfully written to storage and appropriate backup procedures have been completed.

5.12 Backup and system recovery

Effective procedures for the backup of files 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 data. It is vital that backup data include 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 off-site 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 data might be important in the event of a dispute over authenticity. It can be argued that backup media had been compromised, and then used to recover from an information loss, thus affecting the authenticity of stored information. In some cases, the availability of backup data which have been in secure storage, to be used only in the event of a challenge to the authenticity of the live data, can be used to enable the demonstration of authenticity of the stored information.

Facilities on the system should allow for the backup and verification of all files 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 structure of the files held on a backup is different to that of the originals, the structure of the backup files should be detailed in the Systems Description Manual.

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

Procedures for checking that file integrity has not been compromised after a restore should be documented.

Where backup data is used to recover from a system failure, procedures should be documented to ensure that file integrity 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.

5.13 System maintenance

5.13.1 General

The trusted document management 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 integrity of the data captured or created by or stored within it 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 be maintained.

Preventative maintenance should be carried out regularly, in accordance with the supplier's recommendations.

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.

5.13.2 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.

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.

5.14 Security and protection

5.14.1 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 document management 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 file servers, storage, etc.) should be installed in secure areas (as defined in the organization's security procedures), with documented restricted access.

5.14.2 Encryption keys

Encryption techniques can be used to improve the security and integrity of stored data. A complete electronic file can be encrypted so that the information it contains cannot be retrieved without the use of an encryption 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.

5.15 Use of contracted services

5.15.1 General

Specialist service providers are often used for 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 Technical Report, 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 are intended to ensure:

— that where work is carried out by a service provider, the procedures for the demonstration of authenticity of the resulting information 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.

5.15.2 Procedural considerations

In ideal circumstances, where the service provider can demonstrate the implementation of procedures which comply with the Document 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 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 input material 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 material than the client's procedures.

— The client should check that, where the material 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 material 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 whilst they are away from the client's premises.

5.15.3 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 material 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 material being shipped should be adequately packed to avoid risk of damage in transit.

The recipient should promptly check received material 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 material was 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 material. The same process should be implemented on receipt of returned material.

5.15.4 Use of trusted third party

A secure means for detecting any tampering with a data file, or for verifying the contents of a file, is to store a copy of the file with a trusted third party.

If such an approach is taken, an authenticated copy of the electronic file 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 storage of information as recommended by this Technical Report, 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 information they are storing.

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

5.16 Workflow

Some document management 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 data (databases, audit trails, etc.) held on the workflow system should be reviewed for retention requirements and, where applicable, stored in compliance with the Document Management Policy Document.

Where changes to the workflow system are implemented, change control procedures should be implemented to ensure that stored information 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.

5.17 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 integrity and authenticity of a time stamp and its binding to a particular piece of information should be documented.

5.18 Version control

5.18.1 Information

In some applications, digital documents might be subject to change. Typical of such applications are those implemented for controlling technical drawings in drawing offices. Several different versions of a digital document can develop over a period of time, each document being allocated a version number. It is important in such applications to maintain each version as a separate digital document, and also maintain the link between the versions.

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

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

5.18.2 Documentation

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

Superseded versions should be kept for at least the same length of time as that for which relevant information 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 done, there is a risk that the integrity of the information 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 authenticity and integrity of the information.

5.18.3 Procedures and processes

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

5.19 Maintenance of documentation

Compliance with the Document 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 information, 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 vital 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 information 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 document management system, subject to the same controls as included in this Technical Report, 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.

6 Enabling technologies

6.1 General

This clause deals with technology-related topics which are relevant to this Technical Report, including:

— System Description Manual (see 6.2);

— storage media and sub-system considerations (see 6.3);

— access levels (see 6.4);

— system integrity checks (see 6.5);

— image processing (see 6.6);

— compression techniques (see 6.7);

— form overlays and form removal (see 6.8);

— environmental considerations (see 6.9);

— migration (see 6.10);

— information deletion and/or expungement (see 6.11).

6.2 System Description Manual

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

Details of system configurations should be documented.

Details of all changes to the 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 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 system as it was at a particular time in the past.

For systems already in operation, information stored in the system prior to the achievement of compliance with the Document 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 storing that information.

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

6.3 Storage media and sub-system considerations

The risk of stored electronic objects 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 are used, it is not normally possible to modify electronic files once stored, as any such modification would have the effect of destroying at least some data, resulting in files being corrupted, if not made totally irretrievable. Conversely, in the case of systems which use on-line storage, unauthorized modification, which is typically managed by access control, can never be totally guaranteed.

Electronic objects 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 files requires read-write access, and well-designed systems have controls to prevent unauthorized read-write access. Users with read-only access are unable to modify the files. This alone is unsatisfactory unless the system also maintains a secure record of all read-write accesses. In a system where there are very frequent file 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.

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 file that is modified is not the last file stored on the medium, then all following files need 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 on-line is important.

The point in the application processes at which electronic files are 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 files, users should conduct random checks to verify that files which have been frozen have not been altered or removed.

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

6.4 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 stored information.

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

6.5 System integrity checks

6.5.1 General

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

A suitable approach is to utilize a checksum calculated immediately after the information has been captured. This technique ensures that any errors in file 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 information 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 if the checksum algorithm were known. To deal with this eventuality, other procedures are required. A simple method is to write each checksum to the audit trail after calculation.

To protect stored information 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.

6.5.2 Digital and electronic signatures (including biometric signatures)

Digital and electronic signatures offer the possibility of demonstrating that retrieved information is exactly what was stored. 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 electronic file. In some cases, the retriever might use the signature to verify the identity of the original signatory and, with some signature systems, the integrity of the file. 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 integrity of a received file 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 electronic information should include a checksum or hash value embedded in the file and/or stored in a secure system bound to the original information.

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 authenticity of an electronic file, signatures can be used as evidence in demonstrating that any file stored or received by transmission contains the same information as the original file. Processes to be implemented where a query is raised about the authenticity of a file containing a digital signature should be documented.

6.6 Image processing

To provide optimum image output, or to improve recognition rates for an automated data capture process, post-scanning processes can be performed. 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 file. 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 6.8).

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 integrity of the image as a true facsimile of the original. To check that any image processing does not affect the integrity 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.

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 a digital 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 authenticity 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 integrity of a stored image, consideration should be given to also storing the original (e.g. unprocessed) image.

6.7 Compression techniques

The use of file compression techniques should be in accordance with the Document Management Policy Document. Such techniques can be applied to electronic files prior to or during storage, to reduce the file size and 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 file or its related data, or via 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, a decompressed electronic file will not be identical to the original file. This might make the demonstration of integrity of such files more difficult. For example, on an image file, parts of text or drawings might be removed, being replaced by artificially generated data. 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 files should be compared with the originals to check that there is no significant loss of information.

If lossy compression techniques are used, the compression ratios achieved should be documented.

The compression ratio should be chosen, where possible, so that all information that is required within the application context is present in the decompressed file.

The maximum compression ratio acceptable can be determined via the sample set of originals, and can vary between documents in the sample set. It might be necessary to decide whether to use different compression ratios for different documents or to use a single ratio for all documents. If the latter approach is adopted, this will usually mean that the average image file size will be higher, but the speed of processing will also be higher because of reduced operator intervention.

Where it is important that there be no loss of information in a scanned image other than that due to the scanning resolution, lossy compression should not be used. Examples of digital documents for which compression using lossy techniques is not recommended include radiographs (i.e. medical and engineering X-ray images).

Where compression is used, the system should provide adequate facilities, preferably via automated means, to ensure that the requirements for quality control (e.g. checking of image quality after scanning – with ability to rescan if necessary, control over associated data accuracy, control over data integrity) on the compressed file can be met.

6.8 Form overlays and form removal

Where an original document consists of a form with overlayed information, the form can be electronically removed from the scanned image prior to storage (form removal).

Where an electronically removed form is held separately from the scanned images to which it relates, it should be controlled as if it is part of the scanned image.

A record should be retained that the resulting image (without the form) has been the subject of form removal and an identifier of any template used for that removal should also be retained. This information should be stored in conjunction with the resulting image. A copy of any template used should also be stored.

A facsimile made by merging the template with the stripped form might not be a true facsimile of the original, although it can be sufficiently accurate for application use.

The authenticity of such a merged image can be difficult to demonstrate, particularly where misalignment of the form and the overlayed information is evident on the merged image.

It might be appropriate to retain true facsimiles of the original forms, by retaining the originals, making a microfilm copy or retaining a complete image of the form.

6.9 Environmental considerations

A description of the hardware manufacturer's recommendations for the operational environment of all components of the system and of storage media should be documented.

Media handling and storage procedures should also be documented.

All types of storage media have a finite life. In order to ensure that stored information is retrievable, regular checking of the media in accordance with the manufacturer's recommendations is necessary. Procedures for checking the condition of the media should be documented. Media should be checked regularly in accordance with the media manufacturer's recommendations.

6.10 Migration

Information can be stored for a considerable length of time and, importantly, for longer than the lifetime of the current technology. Thus, to ensure the integrity of stored information, it is important to plan from the outset that it might be subject to migration processes. Such processes might involve a change of media and/or change of computer hardware and/or software.

A reliable methodology for dealing with this potential problem is to ensure that electronic files are stored in an industry standard format, or that viewers for each stored format are maintained.

There should be provision for migrating electronic files, including metadata, index data and audit trails, to new technology without loss of integrity, and with sufficient migration process documentation to allow the integrity of the stored information to be established at any time in the future.

6.11 Information deletion and/or expungement

It might be necessary to delete/expunge specific information from trusted document management systems, for instance to comply with a legal or regulatory requirement.

Sometimes, circumstances might require that information scheduled for deletion under its normal retention schedule is not to be deleted at that time. There should be processes in place which can ensure information destruction review prior to destruction, so that these special instances can be accommodated.

Where information is stored on WORM media, deletion of specific information is not possible (unless a controlled process of selective copying to new media is implemented). In some applications, it might be accepted that removal of all index references to the information being deleted is, in practical terms, deletion of the information itself. In some applications, it might be acceptable to mark information as deleted. Where necessary, organizations should check that the implemented procedure is acceptable to the appropriate authority. Care should be taken with such processes, as in some circumstances there might still be a requirement to retrieve this “deleted” information.

When positive removal of information from the system is required, the identification and deletion of all copies of the information (including backup media) will ensure that the necessary action is taken.

The trusted document management system should have facilities to delete or expunge information using an auditable process.

Where deletion and/or expungement is implemented, appropriate authorization should be obtained prior to the action being implemented.

The trusted document management system should have the facility to amend incorrect information or remove unwanted information.

Where amendment or deletion is performed in compliance with legislation, suitable records should be kept to enable compliance with the legislation to be demonstrated.

For more advice on deletion from write-once systems, see ISO/TR 12037.

7 Audit trails

7.1 General

7.1.1 Audit trail data

When preparing information for use as evidence of a transaction or event, it is often necessary to provide further supporting information. This information can include details such as date of storage of the information, details of movement of the information from medium to medium, and evidence of the controlled operation of the system. These details are known as audit trail information. The audit trail as described in this Technical Report consists of the aggregate of the information necessary to provide a historical record of all significant events associated with stored information and the trusted document management system. These details can be split into two categories:

— system;

— stored information.

Records should be kept of trusted document management system historical activities or events that might need to be reconstructed in the future, in support of stored information.

Audit trails should contain sufficient and necessary information to enable the demonstration of the authenticity of stored information.

There are frequently a number of departments (or individuals) within an organization (or external to the organization) who might need to access audit trail information, including those representing user, audit and legal functions.

The content of the audit trail should be agreed upon with all relevant departments within the organization.

In most organizations, the audit trail will consist of a collection of system- and operator-generated logs.

The audit trail should contain data about changes to the information stored on the system.

7.1.2 Creation

Audit trail data should, as far as is practicable, be generated automatically by the system, and the System Description Manual should describe the processes.

In the case of audit trail data not generated automatically by the system, the procedures for generating such data should be documented in the Procedures Manual. Consideration should be given to the scope of each audit trail. For example, where a particular piece of information is created in draft form, and progresses through many drafts, does each draft require a full audit trail, or just the final document?

Automatic audit trails are preferable, as they are easier to manage and authenticate. Where automatic audit trails are not available, the resources needed to create an automated process should be carefully reviewed.

Procedures to be followed when an audit trail data file becomes full (and the identification of this situation) should be documented in the Procedures Manual.

7.1.3 Date and time

Each audit trail data record should have an associated date and time, which relates to the date and time of the event being stored.

The date and time of the event that is stored should be sufficiently accurate that a subsequent investigation can determine the train of events.

In the case of audit trail data that are system-generated, the data should be created immediately following the event that is being documented.

The date and time will normally be that of the creation of the audit trail data, but if this creation is made essentially contemporaneously with the event that is being documented, the time will be to all intents and purposes that of the event itself.

In the case of audit trail data that are generated manually, it should be created as soon as possible after the event that is being documented. For example, if the record is of when an operator started work, document the fact at that time. If the record is of when preparation of a particular batch of paper documents was started, document the fact just before the preparation of that batch commences.

Where the actual time that an event occurred is important, the use of trusted time should be considered.

7.1.4 Storage

The storage of audit trail data is a topic often not included in an organization's document management policies. As they are frequently created automatically, and rarely accessed, they are forgotten, and thus not subject to adequate control.

Some systems control the size of audit trail data files by the use of looping, which sets the maximum size for the data file, and when this size is reached, new data overwrites the oldest data in the file. Thus, old audit trail data are lost.

Audit trail data should be included as a specific document type in the Policy Document.

Audit trail data should be stored for at least as long as the information to which it refers.

7.1.5 Access

Audit trail information needs to be accessed by relevant operators at relevant times. In some applications, access might only be needed on an ad hoc basis, and thus it is important that the access and interpretation procedures are documented.

The Procedures Manual should describe how the audit trails can be accessed and interpreted.

Audit trail data should be available for inspection by authorized external personnel (such as auditors) who have little or no familiarity with the system.

7.1.6 Security and protection

If the authenticity of stored information is questioned, the integrity of the audit trail can be fundamental in establishing the authenticity of the stored information. The audit trail should be kept at the level of security appropriate to preventing any change to any data within it.

Audit trail data should be stored securely in accordance with the relevant Information Security Policy. The audit trail should be subject to internal records management procedures at least as good as other vital records of the organization.

Secure backup copies of the audit trail should be kept. This applies to audit trail data kept on electronic media and on paper/microfilm.

Audit trail information kept within the trusted document management system should not be modifiable. Where file recovery procedures have been implemented, sufficient audit trail data should be stored to demonstrate that the recovery did not affect information authenticity.

For least risk, store audit trail data on WORM media. If a rewritable medium is used, then additional procedures need to be implemented to prevent changes being made. The use of magnetic tape will make it relatively difficult to modify data, as magnetic tape is normally a serially written medium.

If the possibility exists that the audit trail data could be modified, it will be more difficult to establish the authenticity of any information to which these trails apply.

Paper documents used for audit trail data should be frequently removed from the place of use and stored securely. The longer a document that is used for audit trail data (e.g. operator logs) is left in a relatively insecure place, for example at a workstation, the higher the risk of tampering. Users need to assess such risk when using paper for audit trail records. Where paper documents are used, storing copies of them on the trusted document management system is recommended.

See also 7.2.3 for protection over long time periods, by the use of migration or other techniques.

7.2 System

7.2.1 General

These records include details on the following topics:

— audit trail information;

— migration and conversion.

7.2.2 Audit trail information

For all system audit trail data, it should be possible to identify the process involved and the date and time of the event.

Depending on its importance, date and time information can be stored on a batch (where relevant) or individual event basis. Where audit trail data are manually stored by an operator, it might be impractical and unnecessary to create audit trail data on a per-document basis. For example, when undertaking paper document preparation for scanning, it might be sufficient to document the time at which preparation of a batch of documents started and ended; it can suffice to document simply when the operator started and ended work, provided it is possible to identify subsequently which operator prepared which documents.

7.2.3 Migration and conversion

Where information is moved from one storage device to another, as part of a migration process, details of the move should be stored in the audit trail.

Procedures for migration or conversion should include methods by which it can be demonstrated that any related data (such as metadata) are also migrated or converted.

In the case of Hierarchical Storage Management systems (HSMs), where data are routinely and automatically moved between storage devices, without user intervention, it might not be necessary to generate audit trail data on these movements of information. However, it might be necessary to demonstrate that the HSM was working normally when information was transferred.

Where information has been converted from one file format to another, details of the conversion should be stored in the audit trail. For example, a digital document created by a word processor program can be converted to an image format without changing the text within the document. From one perspective, this might be considered not very different from copying a file, but if formatting is relevant to the information content, there is the possibility that the information content of the converted file can be considered to have changed.

7.3 Stored information

7.3.1 General

These records include details on the following topics:

— information capture;

— batch information;

— indexing;

— change control;

— use of digital signatures;

— destruction of information;

— workflow.

7.3.2 Information capture

7.3.2.1 General

Audit trail data about the capture process provides invaluable information to assist in the authentication of stored information. Details such as capture time, operator, capture device and type of original can prove vital when authenticity is challenged.

Information should be kept in the audit trail of key information concerning information captured by or imported into the system. Sufficient information should be stored relating to each processing procedure.

Information that can be stored in the audit trail will typically include:

— document or file identification;

— process date and time stamp;

— batch reference (for batch input);

— number of pages (for document scanning) or data records (data capture);

— quality control check approval;

— an identifier for each document or file that was indexed;

— operator or workstation identifier;

— final write to storage.

The choice of actual data to be stored in the audit trail will depend upon the application and the system.

7.3.2.2 File information

Information can be captured by the system on a file-by-file basis. This is particularly true where electronic files are imported into the system. Where information is captured on a file-by-file basis, the following audit trail information should be stored:

1) unique file identifier;

2) number of documents/pages within the file;

3) size of the file (e.g. kilobytes);

4) file format;

5) file code (for example EDI values, DTD, etc.).

7.3.2.3 Scanned document information

Information can be captured by the system by the scanning of original documents.

Where document scanning is involved, the following audit trail information should be stored:

1) unique internal document identifier;

2) number of page images scanned;

3) number of pages sent to storage device.

7.3.3 Batch information

a) Where data are captured on a batch basis, particularly in document scanning applications, the following audit trail information should be stored:

   1) unique batch identifier;

   2) operator identifier;

   3) type of material scanned, e.g. paper documents, roll microfilm, aperture cards;

   4) quantity of material in the batch, e.g. number of documents, number of pages (single/double sided), number of microfilm frames;

   5) details of image processing performed during the scanning processes, where this is different from any default imaging processing described in the System Description Manual.

b) Audit trail data should be stored so that it is easy to check:

   1) that all required activity has been performed for that batch;

   2) details of any anomalies or discrepancies that have been encountered;

      EXAMPLE Number of pages written to storage not agreeing with number of pages scanned;

   3) that quality control procedures have been completed;

   4) that required exception processing has been completed.

7.3.4 Indexing

Indexing information is vital to the information retrieval process, and thus its accuracy is key to establishing the authenticity of stored information. Audit trail information detailing the creation and modification of indexes can be used to demonstrate that indexing procedures have been correctly utilized.

Information should be kept in the audit trail detailing the date and time of the creation, amendment and deletion of every index file. Audit trail data should include an identifier for each document or data file that is indexed.

Where index data can be amended or deleted, audit trail data should be generated. If an index is being amended, details of the amendment can also be stored.

Where an index item relates to deleted or expunged information, this fact should be documented.

7.3.5 Change control

Where a change is made to stored information, audit trail data should be created and stored, identifying the nature of the change and the person who, or the program (where the change was made automatically by the system) that, initiated the change.

Where appropriate, previous versions of the information should be referenced in the audit trail data, to identify the nature of the change.

7.3.6 Digital signatures

Where digital signatures (or other electronic signing techniques) are used, audit trail data should be kept as follows:

1) file identification;

2) certification of identification;

3) authenticating authority identification;

4) date and time of signature;

5) return receipt/confirmation;

6) proof of validation.

7.3.7 Destruction of information

Audit trail data should be kept of the destruction of paper documents following document scanning. Audit trail data should be kept of the destruction of information at the end of the relevant retention period. Audit trail data should be kept of the authorization for destruction.

7.3.8 Workflow

There should be a record, for audit trail purposes, each time a new business process is defined, or an existing definition is changed.

Where workflow systems are in use, audit trail points should be defined at which audit trail data should be generated.

In most workflow systems, an audit trail point exists at each step in the workflow. However, for compliance with the Policy Document, audit trail information might not need to be kept for every audit trail point. The user should decide which audit trail points are relevant with regard to the potential evidential importance of the data within the workflow. These audit trail points should be selected for the generation of audit trail data.

The selected audit trail points can change as the workflow processes are changed.

The system should permit an authorized user to select and de-select the audit trail points for which audit trail data are generated.

Bibliography

[1] ISO 2859-1 *Sampling procedures for inspection by attributes — Part 1: Sampling schemes indexed by acceptance quality limit (AQL) for lot-by-lot inspection*

[2] ISO 9000, *Quality management systems — Fundamentals and vocabulary*

[3] ISO/TR 12033, *Document management — Guidance for the selection of document image compression methods*

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

[5] ISO 12651, *Electronic imaging — Vocabulary*

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

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

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

[9] ISO/TR 18492, *Long-term preservation of electronic document-based information*

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

[11] The Sedona Principles: *Best Practices, Recommendations & Principles for Addressing Electronic Document Production*

[12] The Sedona Conference Glossary for E-Discovery and Digital Information Management

ICS 37.080

Price based on 41 pages