



Canadian
General
Standards
Board

CAN/CGSB-72.11-93

Supersedes CAN/CGSB-72.11-M88

WITHDRAWN / RETIRÉE

Microfilm and Electronic Images as Documentary Evidence

National Standard of Canada

Canada



The CANADIAN GENERAL STANDARDS BOARD (CGSB), under whose auspices this National Standard of Canada has been developed is a government agency within Public Works and Government Services Canada. CGSB is engaged in the production of voluntary standards in a wide range of subject areas through the media of standards committees and the consensus process. The standards committees are composed of representatives of relevant interests including producers, consumers and other users, retailers, governments, educational institutions, technical, professional and trade societies, and research and testing organizations. Any given standard is developed on the consensus of views expressed by such representatives.

CGSB has been accredited by the Standards Council of Canada as a national standards-development organization. The standards that it develops and offers as National Standards of Canada conform to the criteria and procedures established for this purpose by the Standards Council of Canada. In addition to standards it publishes as national standards, CGSB produces standards to meet particular needs, in response to requests from a variety of sources in both the public and private sectors. Both CGSB standards and CGSB national standards are developed in conformance with the policies described in the CGSB Policy Manual for the Development and Maintenance of Standards.

CGSB standards are subject to review and revision to ensure that they keep abreast of technological progress. Suggestions for their improvement, which are always welcome, should be brought to the notice of the standards committees concerned. Changes to standards are issued either as separate amendment sheets or in new editions of standards.

An up-to-date listing of CGSB standards, including details on latest issues and amendments, and ordering instructions, is found in the CGSB Catalogue, which is published annually and is available without charge upon request. An electronic version, ECAT, is also available. More information is available about CGSB products and services at our Web site — <http://www.pwgsc.gc.ca/cgsb>.

Although the intended primary application of this standard is stated in its Scope, it is important to note that it remains the responsibility of the users of the standard to judge its suitability for their particular purpose.

The testing and evaluation of a product against this standard may require the use of materials and/or equipment that could be hazardous. This document does not purport to address all the safety aspects associated with its use. Anyone using this standard has the responsibility to consult the appropriate authorities and to establish appropriate health and safety practices in conjunction with any applicable regulatory requirements prior to its use. CGSB neither assumes nor accepts any responsibility for any injury or damage that may occur during or as the result of tests, wherever performed.

Attention is drawn to the possibility that some of the elements of this Canadian standard may be the subject of patent rights. CGSB shall not be held responsible for identifying any or all such patent rights. Users of this standard are expressly advised that determination of the validity of any such patent rights are entirely their own responsibility.

Further information on CGSB and its services and standards may be obtained from:

The Manager
Standardization Information Division
Canadian General Standards Board
Ottawa, Canada
K1A 1G6

The STANDARDS COUNCIL OF CANADA is the co-ordinating body of the National Standards System, a federation of independent, autonomous organizations working towards the further development and improvement of voluntary standardization in the national interest.

The principal objectives of the Council are to foster and promote voluntary standardization as a means of advancing the national economy, benefiting the health, safety and welfare of the public, assisting and protecting the consumer, facilitating domestic and international trade, and furthering international co-operation in the field of standards.

A National Standard of Canada is a standard which has been approved by the Standards Council of Canada and one which reflects a reasonable agreement among the views of a number of capable individuals whose collective interests provide, to the greatest practicable extent, a balance of representation of producers, users, consumers and others with relevant interests, as may be appropriate to the subject in hand. It normally is a standard that is capable of making a significant and timely contribution to the national interest.

Approval of a standard as a National Standard of Canada indicates that a standard conforms to the criteria and procedures established by the Standards Council of Canada. Approval does not refer to the technical content of the standard; this remains the continuing responsibility of the accredited standards-development organization.

Those who have a need to apply standards are encouraged to use National Standards of Canada whenever practicable. These standards are subject to periodic review; therefore, users are cautioned to obtain the latest edition from the organization preparing the standard.

The responsibility for approving National Standards of Canada rests with the:


Standards Council of Canada
45 O'Connor Street
Suite 1200
Ottawa, Ontario
K1P 6N7

How to order **CGSB** Publications:

- by telephone — (819) 956-0425 *or*
— 1-800-665-CGSB
(Canada only)
- by fax — (819) 956-5644
- by mail — CGSB Sales Centre
Ottawa, Canada
K1A 1G6
- in person — Place du Portage
Phase III, 6B1
11 Laurier Street
Hull, Quebec
- by email — ncr.cgsb-ongc@pwgsc.gc.ca
- on the Web — <http://www.pwgsc.gc.ca/cgsb>

MICROFILM AND ELECTRONIC IMAGES AS DOCUMENTARY EVIDENCE

Prepared by the
Canadian General Standards Board 

Approved by the
Standards Council of Canada 

Published October 1993 by the
Canadian General Standards Board
Ottawa, Canada K1A 1G6

©Minister of Supply and Services Canada — 1993

No part of this publication may be reproduced in any form without the prior permission of the publisher.

CANADIAN GENERAL STANDARDS BOARD

COMMITTEE ON MICROGRAPHICS AND IMAGE MANAGEMENT

(Membership at date of approval)

Dodson, S.	<i>(Chairperson)</i>	University of British Columbia
Andrews, M.		Command Records Services Ltd.
Appleton, R.		Kodak Canada Inc.
Ardern, C.		CIBC -- Archives/Records
Bookbinder, M.		Optimation International
Butler, D.		Electronic File Imaging Systems Inc.
Chasse, K.		Consultant
Chauncey, C.		Ryerson Polytechnical Institute
Davis, R.G.		Data Repro Com Ltd.
Day, P.		Genealogical Society of Utah
Dempster, G.		Canon Canada Ltd.
Dobkowicz, S.		Royal Bank of Canada
Donoahue, D.F.		Canadian Information and Image Management Society
Gingras, S/Sgt M.		Royal Canadian Mounted Police
Gosson, D.		3M Canada Inc.
Grenkie, R.		Coopers and Lybrand Consulting Group
Guay, Y.		Department of Supply and Services
Hall, S.J.		National Archives of Canada
Hastie, D.		Ontario Hydro
Holinski, D.		M.J. Systems
Knight, S.		Access Systems Ltd.
Lowes, W.		Filenet Canada Inc.
Mackeigan, C.		National Research Council of Canada
Marks, H.		Digital Equipment of Canada
Martel, N.		Canadian Bankers Association
O'Shea, M.		Arenburg Consultants
Postalian, G.		IBM Canada Ltd.
Proulx, P.D.		Solicitor General of Canada
Steel, A.		Autodesk Canada Inc.
Swenson, R.		Department of National Defence
Trowbridge, R.		Bell and Howell Ltd.
Walker, B.		Department of National Defence
Weston, G.I.		Consultant
Wood, D.A.		Public Service Alliance of Canada
Zimmerman, A.		Ontario Ministry of Consumer and Commercial Relations
Melski, T.	<i>(Secretary)</i>	Canadian General Standards Board

Alternate Members:

Baretto, F.	Coopers and Lybrand Consulting Group
Cunningham, R.	Kodak Canada Inc.
Donoahue, J.	Canadian Information and Image Management Society
Gross, B.	IBM Canada Ltd.
Gurushanta, V.S.	Royal Bank of Canada

CGSB wishes to acknowledge the contribution of the Committee under the jurisdiction of the Canadian Information and Image Management Society, which functioned as a CGSB technical working group, in developing the initial draft of this standard; in particular, Vigi Gurushanta (Committee Chairperson) and Ken Chasse, Don Donoahue, Ray Grenkie, Steve Knight (Subcommittee Chairpersons).

Acknowledgment is made for the French translation of this National Standard of Canada by the Translation Bureau of the Department of the Secretary of State.

CAN/CGSB-72.11-93

FOREWORD

This standard is intended to give only general legal information and not legal advice. The laws referred to in the standard may have been altered after publication of the standard. A lawyer should be consulted for legal advice in regard to applying this standard to any particular information management or record-keeping system or issue.

TABLE OF CONTENTS

Page

Introduction	i
I General	1
1. Scope	1
2. Applicable publications	2
3. Terminology	2
4. Fundamentals of a Micrographics and/or Electronic Image Management Program	9
II Micrographics	11
1. Establishing the Micrographics Program	11
2. Preparation of Documents for Microfilming	12
3. Microfilming Procedures	12
4. Evidentiary Requirements (microfilm)	13
5. Storage and Preservation	15
III Electronic Images	16
1. Establishing the Electronic Image Management Program	16
2. Preparation of Documents for Electronic Image Capture	17
3. Basic Control Objectives	17
4. Evidentiary Requirements (Electronic Images)	21
IV Notes and Explanatory Notes	24
1. Notes	24
2. Micrographic explanatory notes	25
3. Electronic image explanatory notes	27

INTRODUCTION

Images as an information medium are important to the business community and to the government because they offer the potential for reduced storage costs over paper records, increased efficiencies in information retrieval, and accurate reproduction of the original. As well, they may enhance the security aspects of computerized record-keeping by providing less expensive duplicate copies of records. However, there are numerous instances where images are not used to their full potential because of the uncertainty of their being admitted into evidence in court proceedings.

The issue is not whether it is legal to copy records. No law prohibits any organization from copying its own records if it is keeping the source records. Rather, the legal issue is whether an image-produced copy will be as admissible and credible in court proceedings as its source record after that source record has been disposed of.

The business record and banking record provisions of the Evidence Acts require that business records be made "in the usual and ordinary course of business" in order to be admissible as evidence in court proceedings. Therefore the image program must be part of the organization's "usual and ordinary course of business".

The admissibility and credibility of image-produced copies cannot be equal to that of the source records without proper authority to dispose of source records and to keep the organization's permanent records on electronic or micrographic media. In the absence of such authority, a court might find, for example, that although the copying of source records such as paper documents is part of the organization's "usual and ordinary course of business", the disposal of those source records is not. Such a finding might prevent admissibility into evidence of the image-produced copies or greatly reduce their credibility even when they are admissible. In addition, the absence of such authority might give rise to an adverse inference that the source records were disposed of in bad faith.

Copying without the disposal of source records is merely the production of another copy; it is not the creation of a new source record having exclusive authority as the official and authoritative record. That should be the purpose of an image management program. To allow source records to continue to exist after copying is to risk an inference that the copies made from them are not as reliable, secure or accurate as those source records.

As a result, the disposal/destruction of records has been provided for in the certification procedure of this standard. If the procedure outlined (which relies heavily upon the certification of all phases of the program) is properly followed, the labour-intensive step of a one-to-one comparison of the captured images and the source records can be avoided.

It is not sufficient that only people in the legal profession and the judiciary understand the requirements of the law of evidence as it relates to business records. It is also necessary that information-handling experts understand these requirements so that the necessary circumstantial guarantees of reliability, security and accuracy that the law of evidence looks for are built into record-keeping systems at the time they are designed. For these reasons, some guidelines on evidentiary requirements are included in the standard in order to assist organizations to comply with the business document provisions of the Evidence Acts.

It is necessary, therefore, that there be guidelines and procedures to enable an organization to demonstrate to a court, tribunal or inquiry, that it has a credible image management program capable of copying source records accurately, reliably and in a timely fashion without loss of value. Therefore, unless otherwise prohibited by law, an organization's senior management can give authority to dispose of its paper source records and rely exclusively on its captured records in the conduct of every day business. However, this standard is subject to, and does not diminish the authority of those special laws that require that source records be kept for specified periods of time. For example: A retention period imposed by the microfilm or photographic document provision of a Provincial Evidence Act or special requirement imposed by a regulatory agency.

At all times, an organization must be prepared to produce its imaged copies as evidence. This is accomplished by the witness or affidavit evidence specified by the Evidence Acts. The evidentiary requirements for business, banking and photographic documents arise from the Canada Evidence Act, the Evidence Acts and Ordinances of the provinces and territories, the common law, and from any specialized legislation that deals with documents for particular uses. Generally, the Canada Evidence Act applies to matters within federal legislative authority, while the provincial and territorial Evidence Acts and Ordinances apply to matters within provincial and territorial legislative authority. The advice of a lawyer is often necessary to be certain of the applicable legislation.

This standard seeks to provide information-handling experts with general legal information so that the integrity sought by the Law of Evidence is built into automated image record-keeping systems at the time they are designed. For these reasons, guidelines on preparing evidence and witnesses for court are included in the explanatory notes in order to assist organizations in complying with the provisions of the Evidence Acts. However, this standard is not intended to provide legal advice, merely general legal information.

CANADIAN GENERAL STANDARDS BOARD

**MICROFILM AND ELECTRONIC IMAGES
AS DOCUMENTARY EVIDENCE**

Part I: GENERAL

1. SCOPE

- 1.1 This standard provides rules and guidelines for organizations to establish and operate a credible image management program with the ability to demonstrate that the resulting captured images are accurate reproductions of source records.
- 1.2 This standard provides guidelines for the capture of images of business source records and the secure storage of those images. In order to maximize the probability of admissibility and weight given to business records as evidence, this standard recommends that they be stored in secure storage. Because computer output to microfilm (COM) is considered by many to be a source record, many of the certification requirements will not be necessary. When microform systems are used which allow images to be erased, special procedures and/or affidavits that are not described in this standard may be necessary to safeguard the system's integrity and the admissibility and credibility of its records. In these circumstances, specific legal advice should be obtained.
- 1.3 This standard does not describe the processing methods and the technical requirements necessary to apply the rules and quality control guidelines specified in this standard. For that purpose, the publications referred to in Part I, Section 2 should be used. These publications deal with such methods and technical requirements as document indexes, capture resolutions, preparation of source records for capture, capture procedures, image compression, image enhancement, and index data verification.

Part I

2. APPLICABLE PUBLICATIONS

2.1 The following publications are applicable to this standard.

2.1.1 Canadian General Standards Board (CGSB)

CAN/CGSB-72.19 -- Criteria for the Evaluation of Micrographic Service Bureaux.

2.1.2 American National Standards Institute/Association for Information and Image Management (ANSI/AIIM)

MS23 -- Practice for Operational Procedures/Inspection and Quality Control of First-Generation, Silver-Gelatin Microfilm of Documents

MS35 -- Recommended Practice for the Requirements and Characteristics of Original Documents That May be Microfilmed

MS42 -- Recommended Practice for the Expungement, Deletion, Correction or Amendment of Records on Microforms

MS44 -- Recommended Practice for Quality Control of Image Scanners

MS52 -- Recommended Practice for the Requirements and Characteristics of Original Documents Intended for Optical Scanning.

2.2 Reference to the above publications is to the latest issues, unless otherwise specified by the authority applying this standard. The sources of these publications are shown in the Notes section.

3. TERMINOLOGY

The following terminology is applicable to this standard. For further definitions of terms commonly used in referring to micrographics and electronic images, please see AIIM TR2 and ISO 6196. The sources of these publications are shown in Part IV, Section 1.

Part I

3.1 Admissibility

"Admissibility" and "admitted into evidence" refer to the acceptance into evidence by a judge in judicial proceedings, or by the presiding officer at a tribunal or public or formal inquiry, of documentation or information that is produced at such proceedings, tribunals or inquiries.

3.2 Annotation

An addition to the content of a record in a manner that does not conceal or destroy the content of the source record, and is identifiable as an addition to the source record.

3.3 Archival

The term "Archival" has been superseded by "Life Expectancy". (See Part I, par. 3.26.)

3.4 Basic Control Techniques

The techniques that ensure the integrity of the image management program and the systematic supervision of procedures from image capture to disposition and storage.

3.5 Bibliographic Information

An index created by the organization (possibly obtained from the source record) that aids in the retrieval of an image.

3.6 Biographic Information

Information regarding image capture may include the date captured, the time, the operator identification, the capture device identification and location, and details of modification, if any.

3.7 Capture

The creation of an image from a source record.

Part I

3.8 Certificate of Image Authorization

This certificate authorizes the capture and the commitment of the images to secure storage in accordance with the organizational policy, to keep a permanent record thereof. It should include the date, name of the authorizing person and sufficient biographical information to clearly identify the records. This certificate may be a paper document (kept separately), a microfilm, an electronic image or an electronic record stored within the boundaries of secure storage.

3.9 Control Document

A document that is captured via an image management system to provide identification, biographical or technical information.

3.10 Control Objective

The goal of an organization to ensure that the day-to-day activities of its image management system are controlled. Control objectives do not prescribe tools, techniques or procedures, but rather the ultimate goal of applying these tools, techniques or procedures.

3.11 Control Techniques

Techniques (usually specific to an individual technology and/or document management application) that can be employed by an organization to satisfy the requirements of the control objectives.

3.12 Disposal

The destruction, erasure, loss or delivery out of the organization of a source record in the ordinary course of business.

3.13 Document Management System

An information management system that manages the capture, distribution, maintenance, and disposal of source records of an organization in a controlled manner.

3.14 EIM

Acronym for "Electronic Image Management".

Part I

3.15 Electronic Image

(See "Image", Part. I, par. 3.21.)

3.16 Enhancement

Heightening the legibility of a record by various manual or electronic methods in a manner that will not change the interpretation of the record.

3.17 Erasure

Removal of image-related information such that no one can become aware of the deleted record through any automated or manual mechanisms used in the normal course of business.

3.18 Evidence

That body of testimony, documentation and physical objects that will be "admitted into evidence" by a court or tribunal as a proper source for determining facts and making decisions.

3.19 Evidence Acts

The Canada Evidence Act, the Evidence Acts of the provinces, and the Evidence Ordinances of the territories.

3.20 Facsimile

A visual equivalent that contains all significant details from the source record and is a substitute for the source record for all purposes for which it was created or maintained.

Part I

3.21 Image

The representation of a source record that can be used to generate an intelligible reproduction of that record, or the reproduction itself, where:

- a. the reproduction is made with the intention of standing in place of the source record;
- b. the interpretation of the reproduction, for the purposes for which it is being used, yields the same information as the source record; and
- c. the limitations of the reproduction (e.g., resolution, tonal or hues) are well defined and do not obscure significant details.

The source record may be subject to disposal for the purpose of constituting the image as the permanent record.

3.22 Image Management Program

An authorized program following strict control guidelines to achieve specific objectives in the capture, storage, and retrieval of images (including photographic and electronic capture). This may also include the disposal of source records.

3.23 Image Management System

A system of procedures and technological components that operate in an integrated manner to capture, store, index, retrieve, distribute, insert, erase and modify images.

3.24 Index

The bibliographic information created by an organization that enables the retrieval of the image.

3.25 Instant Imaging Updatable Microfilm

Specially-coated films in microfiche format on which images can be developed almost instantaneously after exposure. Images can be modified by superimposing (annotating) information over existing data, completely obliterating (sealing over) recording frames, erasing and leaving blank spaces, or erasing and replacing with other information in the same position.

Part I

3.26 Life Expectancy (LE)

A rating of the life time of recording materials or systems. The number following "LE" is a prediction of the minimum number of years during which information can be retrieved without significant loss if the medium is properly processed, stored, and handled (e.g., LE-100 indicates that information should be retrieveable up to a minimum of 100 years of being in storage). Acetate-based microfilm if processed and stored properly will have an LE of 100 years, polyester-based microfilm 500 years.

3.27 Microfilm Program

An authorized program of microfilming and disposing source records for the purpose of constituting the microfilm as the permanent documentation, all conducted as part of the usual and ordinary course of business.

3.28 Operator Capture Certificate

A record that confirms the image capture of a source record by authorized personnel into a given image management system.

3.29 Original

(See "Source Record", Part I, par. 3.37.)

3.30 Quality Assured Image

An image that has been verified according to quality assurance procedures, providing confidence that the interpretation of the image yields the same data as the source record.

3.31 Quality Assured Image Record

The set of quality assured images which has associated data (e.g., bibliographic and biographic) and the linkage between the image and the associated data that have been verified according to quality assurance procedures and maintained in a manner that provides confidence that the image can be retrieved allowing it to stand in place of the source record.

Part I

3.32 Reasonable Period of Time

A time period that is not excessive given the task to be performed. What is a reasonable period of time should be judged by the need for quality control for the given task.

3.33 Records

The records of the transactions of an organization regardless of the medium.

3.34 Removable Medium

A medium used for secure storage that can be removed from the device that reads or records the image and/or data.

3.35 Retakes

The second-time capture of the source record to supersede or replace the same previously-captured image which is of suspect quality.

3.36 Secure Storage

The storage repositories used to hold quality assured image records during the retention period, in a manner that satisfies all the control objectives set out in Part III, Section 3 (in the case of electronic images), or Part II, Section 3 (in the case of microfilm).

3.37 Source Record

A source record may be:

- a. In relation to a record, the record itself or any facsimile intended by the author of the record to have the same effect.
- b. In relation to a photograph, the negative or any print made from it.
- c. In relation to a record produced by a computer system, any printout or other intelligible output that accurately reproduces, whether in the same or a modified form, the data supplied to the computer system.

Part I

3.38 Supervisory Control Techniques

Procedures undertaken by the organization that ensure that the basic control techniques prescribed in its image management program are consistently and effectively applied.

3.39 Target

A target may be:

- a. Any document or chart containing identification information, coding or test charts.
- b. An aid to technical or bibliographical control that is photographed on the film preceding or following the document.

3.40 Technological Components

These include hardware, software and communications components.

3.41 Transitional Storage

Storage repositories used to hold image and related data records, other than in secure storage.

3.42 Weight (of evidence)

The credibility or probative value of evidence. The weight given to evidence is to be distinguished from its admissibility. A document may be admissible and therefore admitted into evidence, but then be given little weight by the judge or jury that has to decide how much to rely upon it.

4. FUNDAMENTALS OF A MICROGRAPHICS AND/OR ELECTRONIC IMAGE MANAGEMENT PROGRAM

4.1 The following factors are necessary for the implementation of a credible image management program:

- a. The written authority from senior management to establish the image management program.
- b. The program's integration into the usual and ordinary course of business of the organization.

Part I

- c. The written authority for the regular disposal of source records a reasonable period of time after the microfilming or image capture process.
- d. The establishment and documentation of the program's systems and procedures.
- e. Provision for quality assurance (see Part IV, par. 2.1).
- f. Provision for appropriate storage and preservation of storage medium considering its desired retention period.
- g. The program's conformity to all applicable micrographics and electronic image standards set out in Part I, Section 2.

Part II: MICROGRAPHICS

1. ESTABLISHING THE MICROGRAPHICS PROGRAM

- 1.1 Authorization** -- The establishment of a micrographics image management program shall be authorized in writing by the corporate policy of the organization. The authorization shall include confirmation that the program will form a part of the usual and ordinary course of business of the organization. The appropriate signing officer or authority shall:
- a. authorize establishment of the micrographics image management program,
 - b. authorize the records or types of records to be captured,
 - c. authorize the records or types of records to be retained,
 - d. authorize the disposal of source records (see Part IV, par. 2.2), and
 - e. authorize the method of recording and certifying that the activities authorized by these five authorizations were in fact carried out as required.
- 1.2 Responsibility** -- A person, directly named or uniquely identified, shall be designated in writing by senior management to be responsible for the micrographics program. The assigned authority shall be clearly defined.
- 1.3 Service Bureaux** -- If an organization employs an external service bureau to carry out its microfilming program, the organization must be satisfied that the bureau's program provides security for the documents, and adequate certificate and filming procedures. The person responsible for selecting the bureau should obtain or provide an account of the bureau's program and confirm that the bureau's procedures are satisfactory. The bureau's operations should be reviewed from time to time and the register of microfilms should be inspected regularly. These procedures should be carried out for the purpose of ensuring that the microfilm produced in the service bureau is as admissible and credible as if the microfilm were produced in-house (see Part I par. 2.1.1).
- 1.4 Changes in the Program** -- All changes and revisions in the program shall be authorized by management before implementation.
- 1.5 Procedures Manual** -- A manual shall be prepared that describes the operations and specifies the procedures required in the program. It shall identify and record the types or categories of documents to be microfilmed, the micrographic formats to be used (e.g. jackets, microfiche or microfilm), the indexing techniques and the appropriate reduction ratio of each application. It shall describe the microfilming procedures, technical standards to be used, quality control procedures including procedures for COM, storage and

Part II

preservation practices, and the quality assurance auditing system. It shall describe the affidavits required, when they must be completed and by whom. The manual shall be an integral part of the training aspects of the micrographics program (see Part IV, par. 2.3).

- 1.6 **Revisions to the Manual** -- Changes in the systems and procedures shall be documented in the manual with the appropriate authorization. The procedures manual must always be up-to-date because it is the organization's most persuasive evidence of its usual and ordinary course of business. It must be written before litigation. A manual entry that is written after the image management program is challenged can destroy the credibility of the program.

It therefore puts at risk the admissibility and weight of its imaged records, if such an entry is shown to be contrived evidence, or written to justify the challenged procedure, practice or rule.

2. **PREPARATION OF DOCUMENTS FOR MICROFILMING**

Documents are often microfilmed in the order in which they were originally created and maintained. Unless a random file arrangement is used, special care should be taken to retain that order. The images on the microfilm should be identified and indexed to ensure that an individual document or series of documents can be easily located on the film (Part II, par. 4.2.2).

3. **MICROFILMING PROCEDURES**

It is important that microfilming and processing are carried out in a controlled manner. Monitoring the established and documented procedures should be as frequent as necessary to ensure consistent quality. All control documents, including targets, and all entries and records deemed necessary to the operation must be completed. Certificates or affidavits shall be prepared and signed as required. (See Part I, par. 2.1.2 ANSI/AIIM MS23.)

- 3.1 **Integrity of Source Records** -- The whole of the source record with all detail and any imperfections shall be captured on microfilm without alterations or retouching of the source record to improve the legibility.
- 3.2 **Enhancement of Source Records** -- Enhancement of source records shall be properly authorized by the micrographics manager or equivalent. If the legibility of a source record is below the generally accepted threshold, the sequence of microfilming shall be as follows: the unacceptable microimage shall be followed immediately by a certificate stating that the preceding

Part II

document has been enhanced and the process clearly stated, and that the following image is that of the enhanced document. To avoid confusion between the two images during retrieval, the enhanced image should be identified in a manner that does not cover or interfere with any information on the document (see Part IV, par. 2.4).

3.3 Retakes -- In applications where a chronological or batch filing arrangement is used, retakes shall be spliced at the beginning of the applicable roll of film (see Part II, par. 4.2.1). Where a random file arrangement is used, usually in conjunction with a computer assisted retrieval (CAR) system, the retake images shall be reindexed to the subsequent roll of film.

3.4 Inspection of Processed Microfilm -- After development, the microfilm shall be inspected to ensure that the photographic requirements in ANSI/AIIM MS23 and in the organization's procedures manual have been met, and that the documents described and identified on the microfilming authorization certificate and the camera operator certificate, together with appropriate control targets, have been microfilmed as directed.

3.4.1 An inspection report shall then be completed, stating that the microfilm (batch/roll etc.) was inspected, that the bibliographical information was compared to the microfilm authorization certification as well as to the camera operator certificate, and that the described documents were properly microfilmed and that all the necessary control procedures were applied during the process. It should also state that a minimum 5% visual inspection of randomly-selected microfilmed images was performed and that there was no reason to believe that any source records were omitted. It shall be signed and dated by the microfilm inspector.

3.5 Audit -- The person(s) who conduct(s) the quality control and inspection procedures during normal operations shall not be involved in audit activities.

4. EVIDENTIARY REQUIREMENTS (MICROFILM)

At all times an organization must be prepared to produce its microfilm as evidence. This is accomplished by witness or affidavit evidence as specified by the Evidence Acts. The affidavit evidence should include statements that the particular equipment involved (i.e., camera, reader, printer, etc.) was in good operating order at the time of the process, that the microfilm program was properly authorized and that the microfilming and disposal of source records was carried out in the usual and ordinary course of business (see Part IV, par. 2.5).

Part II

- 4.1 **Certificate of Microfilming Authorization** -- This certificate authorizes the filming of source records by the custodian, in accordance with organizational policy in order to keep a permanent record thereof. It should include the date, the name of the authorizing person and sufficient biographical information to clearly identify the source records. It may be filmed with the records or kept separately (see Part IV, par. 2.6).
- 4.2 **Camera Operator Certificate** -- The camera operator should sign a form giving his/her name, the date of filming and certification that the microfilm is a complete record of the source records passed to him/her for filming. The form should be filmed immediately before and after the source records to which it refers. If the certificate of microfilm authorization (Part II, par. 4.1) is filmed, the camera operator certificate need only be filmed at the end of the batch. If a batch of source records fills more than one roll of film, a continuation certificate should be filmed at the end of the first roll and at the beginning of the second, and so on.
- 4.2.1 If there is a change of operator during the production of a roll, the first operator should film his/her certificate immediately after the last source record he/she films, and the next operator should film his/her certificate immediately before the first source record he/she films. If retakes are necessary, the camera operator should complete another certificate before and after the source records and state the reason for re-filming. Retake certificates are not necessary in a random-filed CAR system because the documents are treated as a first-time filming and are reindexed in the new roll of film.
- 4.2.2 In those situations where very special or important source records are filmed, such as contracts or executed documents, a verification process such as a sequential numbering system should be used so that the operator can attest to the fact that all source records intended to be filmed were in fact filmed.
- 4.3 **Updatable Microfiche Systems** -- In the case of microfiche jacket systems and other add-on unit record systems where the original roll of film is cut into strips or individual images and inserted into a unitized holder or carrier, a duplicate roll of film shall be made. This may be accomplished by using a dual filming process or by duplicating the original film that must be accompanied by an appropriate certificate attesting to its authenticity. The second roll of film (which must remain uncut), shall be linked through an indexing system to the jacketed images.
- 4.3.1 In the case of instant image updatable systems using specially-coated films in microfiche format, the source records shall also be filmed in a traditional

Part II

manner using silver microfilm. The resulting roll of film shall be linked through an index to the microfiche images.

- 4.4 **Certificate of Disposal of Source Records** -- Most of the photographic document provisions in the Evidence Acts require proof (which can be in the form of an affidavit or sworn declaration) that the source record was disposed of before a microfilm copy will be accepted as evidence in court. Although proof of disposal is not expressly required by the business and banking document provisions of the Evidence Acts, it should always be expected that proof of an acceptable reason for the absence and replacement of source records will be an aspect of a court's interpretation and application of those provisions.
 - 4.4.1 If the source record has been authorized to be disposed of immediately or shortly after microfilming, the affidavit of disposal may be incorporated into the certificate of microfilming authorization (Part II, par. 4.1). However, it may not be practical to incorporate it with the certificate of microfilming if the source record must be kept for a designated period after microfilming (e.g., business documents under an Evidence Act requiring that the source record be kept for a specified retention period).
 - 4.4.2 In either case, the certificate should identify the source records completely as well as the identifying numbers assigned to the microfilmed images. It should state that the bibliographical information assigned to the source records and the microfilm were compared to the microfilm authorization certificate, the camera operator certificate (including retake certificates), as well as the quality control inspection report, and were all found to be the same documents. It should also authenticate that the source records were subsequently disposed of in accordance with the authorized disposal schedule of the organization, and identify the person in whose presence they were disposed of.
- 5. **STORAGE AND PRESERVATION**
 - 5.1 **Original Microfilm** -- The storage medium and the preservation program should be such that the film can be preserved for the intended life of the record (see Part I, par. 3.3 and 3.26).
 - 5.2 **Duplicate Film** -- To preserve the life of the original microfilm, duplicate microfilms should be made for reference or distribution.

Part III: ELECTRONIC IMAGES

1. ESTABLISHING THE ELECTRONIC IMAGE MANAGEMENT PROGRAM

- 1.1 Authorization --** The establishment of an Electronic Image Management (EIM) program shall be authorized in writing by the corporate policy of the organization. The authorization shall include confirmation that the program will form a part of the usual and ordinary course of business of the organization. The appropriate signing officer or authority shall:
- a. authorize establishment of the EIM program,
 - b. authorize the records or types of records to be captured,
 - c. authorize the records or types of records to be retained,
 - d. authorize the disposal of source records (see Part IV, par. 3.1), and
 - e. authorize the method of recording and certifying that the activities authorized by these five authorizations were in fact carried out as required.
- 1.2 Responsibility --** A person, directly named or uniquely identified, shall be designated in writing, by senior management, to be responsible for the EIM program. The assigned authority shall be clearly defined.
- 1.3 Service Bureaux --** If an organization employs an external service bureau or other outsourcing company to carry out its EIM program in whole or in part, the service bureau must conform to all the paragraphs of this standard and will be held accountable to the organization for adherence to standards as specified in this document.
- 1.4 Changes in the Program --** All changes and revisions in the program shall be authorized by management before implementation.
- 1.5 Procedures Manual --** The procedures manual required by this standard to be written by each organization shall describe the EIM program. The procedures manual shall outline the following:
- a. Type of records to be stored
 - b. Procedures for capture (see Part IV, par. 3.3)
 - c. Procedures for indexing
 - d. Procedures for quality control as set out in the control objectives in Part IV, Section 3 of this standard
 - e. Procedures for retrieval of source record or image
 - f. Procedures for certification and registration
 - g. Procedures for disposal of source records

Part III

- h. Procedures for storage on secure storage
- i. Procedures for ensuring the integrity and security of the image and its index
- j. Procedures for storage of removable medium
- k. Procedures for backup and recovery (see Part IV, par. 3.4)
- l. Procedures for disposal of records from the image management system.

- 1.6 **Revisions to the Manual** -- Changes in the systems and procedures shall be documented in the manual with the appropriate authorization. The procedures manual must always be up-to-date because it is the organization's most persuasive evidence of its usual and ordinary course of business. It must be written before litigation. A manual entry that is written after the image management program is challenged can destroy the credibility of the program. It therefore puts at risk the admissibility and weight of its imaged records, if such an entry is shown to be contrived evidence, or written to justify the challenged procedure, practice or rule.

2. PREPARATION OF DOCUMENTS FOR ELECTRONIC IMAGE CAPTURE

Source records should be prepared for capture in accordance with ANSI/AIIM MS52 (Part I, par. 2.1.2).

3. BASIC CONTROL OBJECTIVES

- 3.1 Part III of this standard has been organized on the basis of control objectives which each organization must meet in order to have a controlled EIM program. The specific control techniques required to meet the control objectives are not specified in this standard. The control objectives addressed in this standard are set out in the following sections of the standard:

Part III

Electronic Image Control Objectives

Control	Image Capture	Image	Index Conversion
Basic Controls			
Completeness	3.1	3.5	3.9
Accuracy	3.2	3.6	3.10
Authorization	3.3	3.7	3.11
Maintenance	3.4	3.8	3.12
Evidentiary Controls			
Audit Trails	--	4.2	--
Supervisory	--	4.3	--
Disposal	--	4.4	--

The EIM program should be designed and implemented so that certain basic control objectives are met. Control objectives state what an organization's EIM program must achieve while control techniques describe how those objectives are achieved. Some control techniques for satisfying control objectives are set out in the explanatory notes (Part IV, par. 3.5 and 3.6).

3.2 Completeness of Capture to Transitional Storage -- All source records authorized for capture on transitional storage shall be processed according to the image management program, and written to secure storage. Basic requirements for achieving completeness of capture are as follows:

- a. Proof that all source records designated for capture were in fact captured
- b. Establishment of set control procedures for retakes or correction of rejected images
- c. Documentation of the date and location/terminal of capture and subsequent corrections.

Part III

- 3.3 **Accuracy of Capture to Transitional Storage** -- Images captured by the image management program to transitional storage shall be captured accurately and reliably. The image recorded on transitional storage shall comprise the whole of the source record(s) in a way that does not compromise its status as a facsimile.
- 3.4 **Authorization of Capture to Transitional Storage** -- All images captured by the system must be authorized as set out in the authorized EIM program.
- 3.5 **Maintenance of Images in Transitional Storage** -- There must be adequate provisions for the maintenance, preservation and confidentiality of images in an EIM program. Such provisions should be described in the procedures manual. Control techniques shall ensure that images captured by the EIM program are not subject to unauthorized alterations.
- 3.6 **Completeness of Conversion of Images to Secure Storage** -- All images captured during the process described in Part III, par. 3.2 shall be completely converted to secure storage. In the event that the initial capture is to transitional storage, then the conversion shall occur within a reasonable period of time.
- 3.7 **Accuracy of Conversion of Images to Secure Storage** -- The conversion process from transitional storage to secure storage shall ensure that the image recorded on secure storage shall comprise the whole of the original in a way that does not compromise its status as a facsimile.
- 3.8 **Authorization of Conversion of Images to Secure Storage** -- The following are requirements for achieving authorization of conversion:
- a. Only images captured within the authorized image management system shall be converted to secure storage.
 - b. The time for conversion must not be excessive, given the task to be performed.
 - c. The time for conversion must also be commensurate with the need for quality control.
 - d. Disposal of source records shall not occur until conversion to secure storage has taken place.

Part III

- 3.9 **Maintenance of Images Converted to Secure Storage** -- Control techniques shall ensure that images captured by the EIM program cannot be lost or damaged through accident or omission. Basic protection for images include protection against:
- a. disasters,
 - b. mischief,
 - c. accidental erasure, and
 - d. annotation or replacement which is not authorized.
- 3.10 **Completeness of Bibliographic and Biographic Information** -- All bibliographic and biographic information required by the EIM program must be captured completely.
- 3.10.1 Specifically, bibliographic information created by the organization for the purpose of locating specific images should be consistent and include any of the following:
- a. Subject matter of the image
 - b. Description of the image
 - c. Classification number
 - d. Location of the image
 - e. Any information concerning reference/transfers or changes to the index
 - f. Cross-referencing information about the image record.
- 3.10.2 Biographic information for locating and retrieving images must have the following to be complete:
- a. Exact date of capture
 - b. Capture device location or identification
 - c. Any details on modifications that took place
 - d. Cross-referencing information.
- 3.11 **Accuracy of Bibliographic and Biographic Information** -- All bibliographic and biographic information captured must be accurate for the purposes for which it is intended (i.e., to locate and retrieve specific images, and to reflect historical data about those images).
- 3.12 **Authorization of Bibliographic and Biographic Information** -- Only authorized bibliographic and biographic information shall be captured in the image management system. Authorization is to be obtained in accordance with the authorized procedures manual.

Part III

- 3.13 Maintenance of Biographic and Bibliographic Information** -- Control techniques shall ensure that the biographic and bibliographic information related to images captured by the EIM program cannot be lost or damaged through accident or omission. Basic protection for biographic and bibliographic information includes protection against:
- a. disasters,
 - b. mischief,
 - c. accidental erasure, and
 - d. unauthorized annotation or replacement.
- 4. EVIDENTIARY REQUIREMENTS (ELECTRONIC IMAGES)**
- 4.1** The image management program must satisfy basic control objectives as described above, as well as evidentiary control objectives. Evidentiary control objectives ensure that the basic control objectives are met.
- 4.1.1** The following comments are based upon the law as it stood at the time of the writing of this standard. Canadian law has yet to decide whether electronic images are either original computer-produced source records, or copies of source records. If originals, they would be subject to the same rules that apply to all other computer-produced records. Canadian law provides no detailed description of the evidence required to ensure that computer-produced records will be treated as credible when they are admitted into evidence in court. Therefore, each record or record-keeping system can have its own unique evidentiary problems.
- 4.1.2** A suggested list of specific points for proof when presenting computer-produced records as evidence is given in the explanatory notes (Part IV, par. 3.7). They are subject to being displaced if the law changes by providing its own list of points for proof, or a detailed description of required evidence. These points provide a method of demonstrating compliance with this standard's prime evidentiary requirement that at all times an organization must be prepared to produce its images as evidence. Therefore, they should be listed in the organization's procedures manual as a means for preparing testimonial and affidavit evidence with which to adduce computer-produced business records as evidence. The capture of biographical information should facilitate that preparation. These points provide a method of implementing this standard's evidentiary requirements in court.
- 4.1.3** If in addition to, or instead of, the evidentiary requirements for computer-produced records, image-produced records are treated as being copies of

Part III

source records (originals), the following additional points might apply. Generally, courts will accept a copy as a substitute for a source record if: 1) the source record is no longer available, 2) the copy was made with the intention of standing in the place of the source record, 3) the absence of the source record is adequately explained, and 4) the circumstances of disposal of the source record and the creation of the copy are adequately explained. Again, the application of these points will vary with the evidentiary problems presented by each record sought to be adduced into evidence, and with the specific legal rules that are applied to them. To go beyond these general statements to more specific statements requires professional legal advice because each record will have its own unique evidentiary problems.

- 4.2 **Audit Trails** --The EIM system shall operate in such a way that the application of basic and supervisory control techniques can be easily proved. Biographic data as to the system operation must be inherent to the operation of the image management program and automatically produced by it, otherwise operator certificates must be used and stored.
- 4.2.1 All authorization functions shall be traceable through controlled bibliographic and biographic information to specific individuals and equipment operating as prescribed in the image management program.
- 4.3 **Supervisory Control Objectives** -- The control techniques employed to satisfy control objectives in Part III, Section 3 shall be subject to additional supervisory control techniques to ensure their continued operation. Basic supervisory control requirements include:
 - a. the appointment of an officer responsible for the integrity of the image management program, and
 - b. the systematic supervision from image capture to disposition and storage.
- 4.4 **Certificate of Disposal of Source Records** -- Most of the photographic document provisions in the Evidence Acts require proof (which can be in the form of an affidavit or sworn declaration) that the source record was disposed of as a condition-precedent to the admissibility of a print from photographic film. Although image-produced documents are not subject to these provisions, similar requirements might be imposed upon them by means of judicial interpretations for other applicable statutory provisions (such as the business document provisions found in most but not all of the Evidence Acts, and/or the banking document provisions found in all of the Evidence Acts), or imposed by other rules of law (such as common law or judge-made law). Therefore, to

Part III

provide evidence using image-produced documents rather than source records, proof of disposal and replacement of the source records by means of a well-regulated image management program will be required.

- 4.4.1 However, if paper source records are required to be kept for a designated period after capture, a separate record of disposal of the paper source records will have to be kept. There are no retention periods specified in the Evidence Acts for image-processed records as there are for microfilmed records. Most of the provincial Evidence Acts require that the source records that have been microfilmed be kept for a fixed period.
- 4.4.2 If they are disposed of before the fixed period, the microfilmed records are subject to the court's discretion as to whether to allow them to be used as evidence, rather than being admissible into evidence as of right. There is no comparable rule for electronic image-processed records. But because of the vagueness and breadth of the language in the Evidence Acts that applies to business documents, comparable requirements could be imposed because of the broad scope of judicial interpretation that that language could support.

Part IV: NOTES AND EXPLANATORY NOTES

1. NOTES

1.1 Related publications -- The following publications are related to this standard:

1.1.1 International Organization For Standardization (ISO)

6196 -- Parts I to VIII -- Micrographics -- Vocabulary.

1.1.2 Association for Information and Image Management

AIIM TR2 -- Glossary of Imaging Technology

AIIM TR25-- The Use of Optical Disks for Public Records

AIIM TR31 -- Performance Guideline for Admissibility of Records as
Evidence Produced by Information Technology Systems (Part 1).

1.2 Sources of Referenced Publications

1.2.1 The publication referred to in Part I, par. 2.1.1 may be obtained from the Canadian General Standards Board, Sales Centre, Ottawa, Canada K1A 1G6. Telephone 1-800-665-CGSB. Fax (613) 941-8705.

1.2.2 The publications referred to in Part I, par. 2.1.2 may be obtained from the American National Standards Institute, 11 West 42nd Street, New York, NY 10036, U.S.A. Telephone (212) 642-4900. Fax 302-1286, or from the Standards Council of Canada, Standards Sales Branch, 45 O'Connor Street, Suite 1200, Ottawa, Canada K1P 6N7. Telephone 1-800-267-8220 or (613) 238-3222. Fax (613) 995-4564.

1.2.3 The publication referred to in Part IV, par. 1.1.1 may be obtained from the Standards Council of Canada, Standards Sales Branch, 45 O'Connor Street, Suite 1200, Ottawa, Canada K1P 6N7. Telephone 1-800-267-8220 or (613) 238-3222. Fax (613) 995-4564.

Part IV

- 1.2.4 The publications referred to in Part IV, par. 1.1.2 and 1.1.3 may be obtained from either the Canadian Information and Image Management Society, 86 Wilson Street, Oakville, Ontario L6K 3G5. Telephone (905) 842-6067. Fax 842-2646, or the Association for Information and Image Management, 1100 Wayne Avenue, Suite 1100, Silver Springs, MD 20910-5699, U.S.A. Telephone (301) 587-8202. Fax (301) 587-2711.

2. MICROGRAPHIC EXPLANATORY NOTES

These notes refer to clauses in the standard as indicated. AIIM TR25 is a related publication.

- 2.1 **Quality Assurance** (Part I, par. 4.1e.) -- Quality assurance involves a series of audits carried out periodically by an independent party to verify that all the control activities of a given program follow all the applicable technical standards and recommended industry practices. It ensures that overall control of the operations is being carried out faithfully and effectively at all stages. The emphasis of quality assurance is on the planning, reviewing and auditing of the goals, objectives and procedures of the overall quality management program (see Part I, par. 2.1.2, MS44).
- 2.2 **Authorization for Disposal of Source Records** (Part II, par. 1.1d) -- If the source record has been authorized to be disposed of immediately or shortly after capture, the affidavit of disposal may be incorporated into the certificate of imaging authorization. If the source records must be kept for a designated retention period after capture, (e.g., business documents under an Evidence Act requiring that the source record be kept for a specified retention period), it may not be practical to incorporate it with a certificate of image authorization.
- 2.2.1 In either case, the certificate should identify the source records completely as well as identify the associated index information. It should state that the bibliographical information assigned to the source records and the imaged copies were compared to the image authorization certificate, the capture operator certificate, as well as the quality control inspection report and all were found to be the same documents. It should also authenticate that the source records were subsequently disposed of in accordance with the authorized disposal schedule of the organization and identify the person in whose presence they were disposed of.

Part IV

- 2.3 **Procedures Manual (Part II, par. 1.5)** -- The procedures manual should state that the following document handling procedures be in place:
- a. Source records must be available for retake until images on transitional storage are quality assured.
 - b. Source records shall not be disposed of until the quality assured image record in question is accurately and completely transferred from transitional storage onto secure storage.
- 2.4 **Procedures for Capture** -- The capture operator should log on, perform quality assurance of equipment (Part I, par. 2.1.2, MS44), and certify that the image file is a complete record of the documents passed to him/her for capture. This log should be a mandatory part of the image management system. If the certificate of image authorization is a paper document and it is captured, the operator need only log completeness at the end of the document batch. If the certificate is an electronic file, it may be electronically logged into the image management system.
- 2.5 **Enhancement of Source Records (Part II, par. 3.2)** -- Documents are not always in ideal condition for microfilming. Age and wear and tear through usage take their toll. However, some organizations are using photocopiers to improve the legibility of poor documents. Photo filters adapted to cameras can also enhance images.
- 2.6 **Evidentiary Requirements (Part II, Section 4)** -- The evidentiary requirements for business documents are outlined in, 1) the Canada Evidence Act, which applies to court proceedings governed by the federal legislation, and 2) in the various provincial and territorial Evidence Acts and Ordinances which apply to matters governed by provincial and territorial legislation.
- 2.7 **Certificate of Microfilming Authorization (Part II, par. 4.1)** -- The capture device operator should sign a certificate giving his/her name and the date of capture and certify that the image is a complete record of documents passed to him/her for capture. The certificate should be captured immediately before and after the documents to which it refers. If the certificate of image authorization is imaged, the operator certificate need be imaged only at the end of the document batch. If a batch of documents is interrupted, for example at the end of a work period, or when more than one roll of microfilm is required, a continuation certificate should be imaged at the end of the first period and at the beginning of the second period, and so on until the batch is completed.

Part IV

3. ELECTRONIC IMAGE EXPLANATORY NOTES

These notes refer to clauses in the standard as indicated.

- 3.1 Authorization for Disposal** (Part III, par. 1.1d) -- If the source record has been authorized to be disposed of immediately or shortly after capture, the affidavit of disposal may be incorporated into the certificate of image authorization. If the source records must be kept for a designated retention period after capture (e.g., business documents under an Evidence Act requiring that the source record be kept for a specified retention period), it may not be practical to incorporate it with a certificate of image authorization.
- 3.1.1** In either case, the certificate should identify the source records completely as well as identify the associated index information. It should state that the bibliographical information assigned to the source records and the imaged copies were compared to the certificate of image authorization, the capture operator certificate, as well as the quality control inspection report, and all were found to be the same documents. It should also authenticate that the source records were subsequently disposed of in accordance with the authorized disposal schedule of the organization and identify the person in whose presence they were disposed of.
- 3.2 Procedures Manual** (Part III, par. 1.5) -- The procedures manual should state that the following document handling procedures should be in place:
- a. Source records must be available for retake until images on transitional storage are quality assured.
 - b. Source records shall not be destroyed until the quality assured image record in question is accurately and completely transferred from transitional storage onto secure storage.
- 3.3 Procedures for Capture** (Part III, par. 1.5b) -- The capture operator should log on, perform quality assurance of equipment (see Part I, par. 2.1.2, MS44) and certify that the image file is a complete record of the documents passed to him/her for capture. This log should be a mandatory part of the image management system. If the certificate of image authorization is a paper document and it is captured, the operator need only log completeness at the end of the document batch. If the certificate is an electronic file, it may be electronically logged into the image management system.

Part IV

- 3.4 **Procedures for Backup** (Part III, par. 1.5k) -- In case of a disaster, it is recommended that a backup copy of the electronic images and the index information be created and securely maintained off-site.
- 3.5 **Completeness of Capture** (Part III, par. 3.2) -- If the electronic image management program's biographical procedures do not automatically record the date, location, terminal and operator of electronic image capture, a certificate containing such biographical data should be completed and signed by the operator. Such biographical data is essential to enable the organization's electronic image management program to fulfil the prime evidentiary requirement of this standard which is that an organization must be prepared at all times to produce electronic image copies as evidence, accompanied by their complete biographical and bibliographical information (except for bibliographical security information about the system that must be kept confidential to maintain the effectiveness of its security procedures).
- 3.6 **Proof of Authorization (Certificate of Electronic Image Authorization)** (Part III, par. 3.8) -- This certificate (paper or electronic file) will authorize the capture of source records by the custodian in accordance with the organizational policy in order to keep a permanent record thereof. It shall include the date, name of authorizing person and sufficient biographical information to clearly identify the documents. It may be captured with the source records or if it is an electronic file, it may be electronically logged into the image management system.
- 3.7 **Evidentiary Requirements (Image) -- Preparing Computer-Produced Business Records as Evidence in Court Proceedings** (Part III, Section 4) -- Here are suggested points of proof with which to cope with the legal uncertainties as to what makes a business document admissible as evidence in the courts. They are subject to being displaced if the law changes by providing its own list of points for proof, or a detailed description of required evidence. There are particular key parts and procedures of all information management and record-keeping systems that information managers and witnesses adducing business records as evidence should incorporate within the testimony that they prepare for court. Because the Evidence Acts expressly direct the courts to consider "the circumstances of the making of records", or "the method and time of preparation", and "the usual and ordinary course of business", testimony to establish system integrity and reliability should cover the whole of the information management and record-keeping process. The following ten points provide a framework for that preparation. They are a consolidation of principles taken from legal writings, including statutes, produced in Canada, the United States, Britain, and other countries. They are principles to be

Part IV

applied when determining the evidence a witness presenting business records should be prepared to give. These points can be used as principles by which to judge the admissibility and weight to be given to computer-produced records. Therefore, they should be listed in the procedures manual in relation to this standard's prime evidentiary requirement in Part IV, Section 3 that an organization must be prepared at all times to produce its electronic image copies as evidence:

- 3.7.1 ***Sources of Data and Information*** -- Proof of the sources of data and information recorded in the databases upon which the record is based. One should be able to describe, at least in general terms, the sources of data and information in one's information or record-keeping system. Information management and record-keeping cannot be more reliable than the quality of the data and information that goes into it.
- 3.7.2 ***Contemporaneous Recording*** -- Proof that the data and information in those databases was recorded in some fashion contemporaneously with, or within a reasonable time after, the events to which such data and information relates (but contemporaneous recording within those databases themselves is not required). The fact that facts and events have not been recorded close to the time when they happened may give rise to an inference that they have been forgotten to some extent or misremembered. Contemporaneous recording removes the possibility of drawing that inference.
- 3.7.3 ***Routine Business Data and Information*** -- Proof that the data and information upon which the record is based is of a type that is regularly supplied to the computer during the regular activities of the organization from which the record comes. Courts look for data and information that comes from regular business transactions, as distinguished from data and information that is unusual to the business, or has been specially contrived for a court case.
- 3.7.4 ***Privileged Data and Information*** -- A certification that the use in court proceedings of the data and information upon which the statements in the record are based does not violate any legal principle of privileged or confidential data and information thereby preventing its disclosure. (This principle would require an assessment of the applicable law of privileged and confidential data and information in relation to a specific business record that is intended to be adduced as evidence.)

Part IV

- 3.7.5 **Data Entry** -- Proof that the entries into the database(s) were made in the regular course of business. (This is another example of the court's use of the principle of "routine business procedure" or "business as usual" as a standard for verifying the reliability of data and information in business records.)
- 3.7.6 **Industry Standards** -- Proof that the input procedure to those databases conforms to standard practices in the industry involved. Although national standards for data processing in general do not yet exist, accepted practices within any part of the industry should be conformed to, so as to prevent the possibility that a court opponent might show that they are not being conformed to. As well, other professional organizations have published important treatises that supply standards.
- 3.7.7 **Business Reliance** -- Proof that there has been reliance upon those databases in making business decisions within a reasonably short time before or after producing the records sought to be admitted into evidence. The credibility of assurances and evidence of reliability of a database can be greatly enhanced by showing reliance upon that database in making business decisions, and showing that such reliance has led to the successful operation of the business that so relies upon that database.
- 3.7.8 **Software Reliability** -- Proof that the computer programs used to produce the output, accurately process the data and information in the databases involved. In other words, demonstrating a history of reliability will nullify arguments of speculative shortcomings and worst-case scenarios. If, however, a history of reliability does not yet exist because the system is too new, its vendor should provide that history from the experience of other customers or suppliers and programmers.
- 3.7.9 **A Record of System Alterations** -- Proof that from the time of the input of the data into the databases until the time of its production, records have been kept by a responsible person in charge of alterations to the system.
- 3.7.10 **Security** -- Proof of the security features used to guarantee the integrity of the total information or record-keeping system upon which the output is based, and of the effectiveness of such features. Security varies with the type of information system and its use so as to produce the appropriate compromise

Part IV

between access and security, between ease of use and accuracy, and between efficiency and cost. Therefore, different systems will implement the following key points of security to differing degrees:

- a. Protecting against unauthorized access to data and to permanent records
- b. Processing verification of data and statements in records
- c. Safeguarding communications lines
- d. Maintaining copies of records on paper, microfilm, or other reliable physical or electronic forms for purposes of verification or replacement of falsified, lost or destroyed permanent and temporary records.

The factors cited in the above ten points should be able to be testified to by a single supervising officer of any well-run information or record-keeping facility, big or small. An additional witness may be required for software that is unique to the system unless that supervisor can testify to its history of reliability. If not, the programmer who wrote it should be available to certify its reliability until it does have a history of reliability. The proper choice of suppliers and programmers requires that consideration be given to their ability and experience in certifying the reliability of their products.

The evidence that these ten points will produce will vary with each information management or record-keeping system. Therefore, the records that each produces for court should be looked upon as creating its own unique evidentiary problems.