Government of Canada | Gouvernement du Canada

Canadian General Standards Board | Office des normes générales du Canada

CAN/CGSB-72.34-2005

Electronic Records as Documentary Evidence

ICS 37.080

National Standard of Canada

Canada

Experience and excellence

Expérience et excellence

CGSB GC

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 Review 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 — www.ongc-cgsb.gc.ca.

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
Strategic Standardization Division
Canadian General Standards Board
Gatineau, 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
270 Albert Street
Suite 200
Ottawa, Ontario
K1P 6N7

NATIONAL STANDARD OF CANADA CAN/CGSB-72.34-2005

ELECTRONIC RECORDS AS DOCUMENTARY EVIDENCE

Prepared by the
Canadian General Standards Board CGSB

Approved by the
Standards Council of Canada

Published December 2005 by the
Canadian General Standards Board
Gatineau, Canada K1A 1G6

CANADIAN GENERAL STANDARDS BOARD

COMMITTEE ON MICROGRAPHICS AND IMAGE MANAGEMENT

(Membership at date of approval)

Gurushanta, V.S.	*Chairperson*	Evida Group
Anderson, P.M.		David Thompson Health Region
Ardern, C.		ARMA International
Bookbinder, M.		Interactive Technologies
Charbonneau, D.		National Defence
Chasse, K.		Legal Advisor
Clyde, A.		Filenet
Davis, R.G.		Data Repro Com Ltd.
Fisher, P.		CLARA
Fortin, J.-Y.		Human Resources and Skills Development Canada
Grush, B.		Realtime Enterprise Group
Knight, S.		Access Systems Ltd.
Knoppers, J.V.		Information Management Services (INFOMAN) Inc.
Knorr, D.		Canada Revenue Agency
Krishnamoorthy, R.		Deloitte & Touche LLP
MacKenzie, D.		Docucom Imaging Solutions
MacLeod, D.		Archives of Ontario
O'Shea, M.		The Information Professionals
Priest, G.		Iron Mountain
Provick, B.		Library and Archives Canada
Roy, B.		Royal Canadian Mounted Police
Sled, T.		MCS Inc.
Steel, A.		Autodesk Canada Inc.
Touchette, F.		Gestion Folio Data
Wold, K.J.		Ministry of the Attorney General, Ontario
Dolhan, P.	*Secretary*	Canadian General Standards Board

Acknowledgment is made for the translation of this National Standard of Canada by the Translation Bureau of Public Works and Government Services Canada.

Contents

Page

Page

Foreword

CAN/CGSB-72.34 specifies principles and procedures for creating all forms of electronic records (text, data bases, e-mail systems, bar code, cartographic, audio, pictorial, multimedia, etc.) to enhance their admissibility as evidence in legal proceedings. Because this standard provides only general legal and technical information, users should seek expert legal and technical advice before applying its recommendations to a specific records management or record-keeping system or to an Electronic Data Interchange (EDI) between autonomous parties.

This standard reflects the ISO/IEC standards and the federal, provincial and territorial acts and regulations in place at the time of Committee deliberations. Where differences exist between an act or a regulation and this standard, the former shall prevail.

0 Introduction

0.1 Context

An organization must always be ready to produce its records as evidence in legal proceedings. To ensure their reliability, integrity and authenticity, organizations should consider the application of standards. To enhance the admissibility and the weight (probative value) of electronic records as evidence in legal proceedings, organizations should apply the principles and procedures outlined in this standard.

0.2 Link to Canadian legal evidentiary requirements

Records and documents including electronic images produced by or stored in a computer can stand in place of original paper source records or copies of paper source records. The legal tests to be met use phrases such as "the integrity of the electronic record system" and "the reliability of the entry." These key phrases are not defined by the law, but the *Canada Evidence Act*, as well as most provincial and territorial evidence acts, contains the following provision, encouraging the use of standards:

> 31.5 For the purpose of determining under any rule of law whether an electronic document is admissible, evidence may be presented in respect of any standard, procedure, usage or practice concerning the manner in which electronic documents are to be recorded or stored, having regard to the type of business, enterprise or endeavour that used, recorded or stored the electronic document and the nature and purpose of the electronic document.

0.3 Sources of requirements and approach

This standard specifies in broad terms the policies, procedures, practices and documentation that organizations need to establish the integrity and authenticity of recorded information as an electronic record in an electronic records management system (RMS). Its technology-neutral language allows organizations to apply the procedures to various types and combinations of Information Technology (IT). The standard provides procedures and practices that will assist them in complying with legal requirements, without dictating the types of technology required.

As a codification of best practices, organizations can rely on this standard if they implement the appropriate procedures and follow them at all times. Applying the standard to an organization's business will not eliminate the possibility of litigation, but it will make the production of electronic records easier and their acceptance in a legal proceeding more certain.

Figure 1 illustrates the various elements considered in drafting this standard and those likely to benefit from its application. See also Annex A.

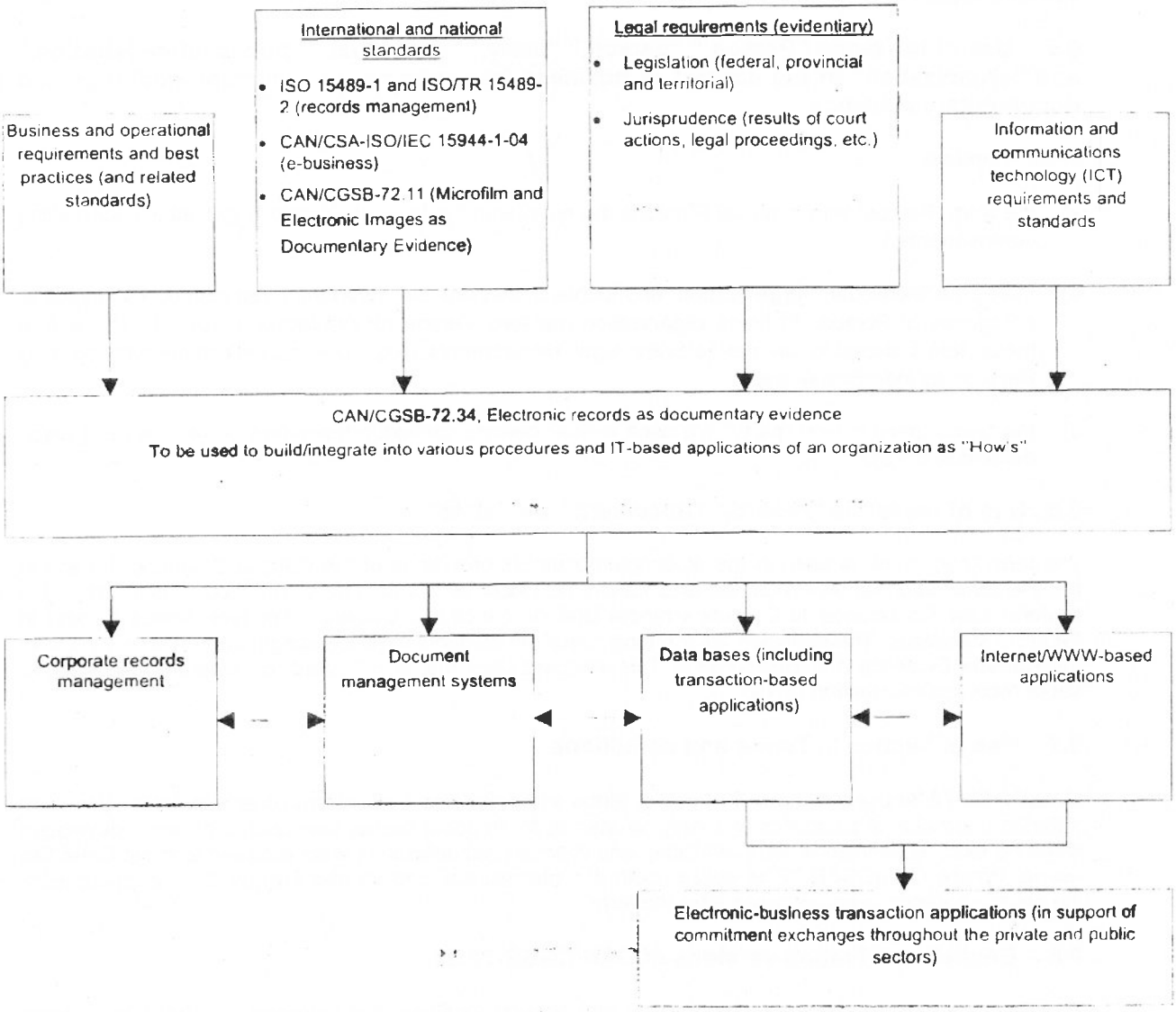

Figure 1 — Framework for the development and the application of CAN/CGSB-72.34

0.4 Applicability of this standard

This standard applies to recorded information and electronic records in IT Systems used by individuals and organizations operating in the private or public sector and on a profit or not-for-profit basis. The standard applies to all types of electronic records.

0.5 Use of the terms "Person," "person," "party," "individual," "public administration," and "organization" in the context of business transactions, commitment exchange and documentary evidence

In this standard

a) the term "Person" with a capital *P* means the entity with the legal ability and responsibility for making commitments;

b) the terms "individual," "organization" and "public administration" mean the three common subtypes or categories of Person. At times organization replaces Person for readability purposes. The use of these terms depends on the relevant legal requirements (e.g., privacy legislation protects only Persons as individuals); and

c) the terms "person" and "party" are used in their generic context independent of the roles of Person defined in 0.5 a).

0.6 Use of the terms "record," "document" and "data"

The term "document" is used in the electronic document provisions of the *Canada Evidence Act* and in the *Personal Information Protection and Electronic Documents Act*. The term "record" is used in the Uniform Law Conference of Canada's model Uniform Electronic Evidence Act (see Annex B) and in ISO/IEC standards. The definition for the term "data" (in evidentiary proceedings) is the same as that of the *Canada Evidence Act*, section 31.8. This standard uses the term "record" or, where appropriate, "a set of recorded information (SRI)."

0.7 Use of Section 3, Terms and definitions

CAN/CGSB-72.34 uses, whenever possible, terms and definitions from international standards, Canadian adopted international standards and national standards. In some cases, new definitions were developed when no existing definitions were available, and international definitions were modified to meet Canadian usage. Where CAN/CGSB-72.34 utilizes both the international English and French of an adopted term, the source appears in parentheses after the term.

0.8 English and French versions of CAN/CGSB-72.34

To ensure agreement between the English and French versions, the following principles have been adhered to. Where the English version utilizes "record," the French equivalent "enregistrement" is used in the French version. Whenever the English version utilizes "document," the French equivalent "document" is used in the French version.

The French version of CAN/CGSB-72.34 differs with the international French for some terms, because of Canadian usage. For example, the terms "disposition," "preservation," "record," and "records management" in the English version are translated as "élimination," "préservation," "enregistrement," and "gestion des enregistrements" respectively.

Electronic records as documentary evidence

1 Scope

1.1 This standard applies to those who receive, create, capture, maintain, use, store or dispose of records electronically. This standard applies to private and public sector activities of Persons irrespective of whether such activities are undertaken on a for-profit or not-for-profit basis.

1.2 This standard is intended for use by those who want to ensure that the recorded information (electronic records and transactions) in their IT Systems is trustworthy, reliable and recognized as authentic. Typical users include

a) managers of private and public sector organizations;

b) IT Systems and records management system (RMS) professionals;

c) all other personnel in organizations, including those responsible for security services and risk management; and

d) legal professionals and other Persons responsible for creating and maintaining records.

1.3 This standard provides principles for developing policies, procedures, practices and documentation for the integrity and authenticity of electronically recorded information to

a) ensure that electronic records can reliably support business decisions and exchanges of commitments;

b) enhance the admissibility and the weight of electronic records in a court of law, a tribunal or an inquiry; and

c) protect the value of electronic records in documenting the content and accountability for decisions and transactions.

1.4 This standard also defines best practices for electronic storage of business or other recorded information. Therefore, organizations conforming to its recommendations benefit even when evidentiary issues are not relevant.

1.5 In addition, this standard provides guidelines for

a) records management supporting a quality process framework; and

b) identifying and implementing appropriate measures to protect the evidentiary value of electronic records, including their incorporation within systems design and management processes.

2 Normative references

2.1 The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

2.2 Canadian General Standards Board (CGSB)

CAN/CGSB-72.11, Microfilm and Electronic Images as Documentary Evidence

2.3 Canadian Standards Association (CSA)

CAN/CSA-ISO/IEC 2382-7-04, *Information Technology — Vocabulary — Part 7: Computer Programming*

CAN/CSA-ISO/IEC 2382-8-01, *Information Technology — Vocabulary — Part 8: Security*

CAN/CSA-ISO/IEC 2382-9-96, *Information Technology — Vocabulary — Part 9: Data Communication*

CAN/CSA-ISO/IEC 2382-16-01, *Information Technology — Vocabulary — Part 16: Information Theory*

CAN/CSA-ISO/IEC 2382-24-96, *Information Technology — Vocabulary — Part 24: Computer-Integrated Manufacturing*

CAN/CSA-ISO/IEC 2382-28-96, *Information Technology — Vocabulary — Part 28: Artificial Intelligence — Basic Concepts and Expert Systems*

CAN/CSA-ISO/IEC 2382-31-01, *Information Technology — Vocabulary — Part 31: Artificial Intelligence — Machine Learning*

CAN/CSA-ISO/IEC 10181-2-00, *Information Technology — Open Systems Interconnection — Security Frameworks for Open Systems: Authentication Framework*

CAN/CSA-ISO/IEC 11179-3-04, *Information Technology — Metadata Registries (MDR) — Part 3: Registry Metamodel and Basic Attributes*

CAN/CSA-ISO/IEC TR 13335-1-01, *Information Technology — Guidelines for the Management of IT Security — Part 1: Concepts and Models for IT Security*

CAN/CSA-ISO/IEC 14662-01, *Information Technology — Open-EDI Reference Model*

CAN/CSA-ISO/IEC 15944-1-04, *Information Technology — Business Agreement Semantic Descriptive Techniques — Part 1: Operational Aspects of Open-Edi for Implementation*

2.4 Department of Justice Canada

Canada Evidence Act (CEA)

Personal Information Protection and Electronic Documents Act (PIPEDA)

2.5 Uniform Law Conference of Canada

Uniform Electronic Evidence Act (UEEA)

2.6 International Organization for Standardization (ISO)

ISO/IEC 2382-1, *Information technology — Vocabulary — Part 1: Fundamental terms*

ISO 2382-2, *Data processing — Vocabulary — Part 2: Arithmetic and logic operations*

ISO 2382-3, *Information processing systems — Vocabulary — Part 3: Equipment technology*

ISO/IEC 2382-4, *Information technology — Vocabulary — Part 4: Organization of data*

ISO/IEC 2382-5, *Information technology — Vocabulary — Part 5: Representation of data*

ISO 2382-6, *Information processing systems — Vocabulary — Part 6: Preparation and handling of data*

ISO 2382-10, *Data processing — Vocabulary — Part 10: Operating techniques and facilities*

ISO 2382-12, *Information processing systems — Vocabulary — Part 12: Peripheral equipment*

ISO/IEC 2382-13, *Information technology — Vocabulary — Part 13: Computer graphics*

ISO/IEC 2382-14, *Information technology — Vocabulary — Part 14: Reliability, maintainability and availability*

ISO/IEC 2382-15, *Information technology — Vocabulary — Part 15: Programming languages*

ISO/IEC 2382-17, *Information technology — Vocabulary — Part 17: Databases*

ISO/IEC 2382-18, *Information technology — Vocabulary — Part 18: Distributed data processing*

ISO 2382-19, *Information processing systems — Vocabulary — Part 19: Analog computing*

ISO/IEC 2382-20, *Information technology — Vocabulary — Part 20: System development*

ISO 2382-21, *Data processing — Vocabulary — Part 21: Interfaces between process computer systems and technical processes*

ISO 2382-22, *Information processing systems — Vocabulary — Part 22: Calculators*

ISO/IEC 2382-23, *Information technology — Vocabulary — Part 23: Text processing*

ISO/IEC 2382-25, *Information technology — Vocabulary — Part 25: Local area networks*

ISO/IEC 2382-26, *Information technology — Vocabulary — Part 26: Open systems interconnection*

ISO/IEC 2382-27, *Information technology — Vocabulary — Part 27: Office automation*

ISO/IEC 2382-29, *Information technology — Vocabulary — Part 29: Artificial intelligence — Speech recognition and synthesis*

ISO/IEC 2382-32, *Information technology — Vocabulary — Part 32: Electronic Mail*

ISO/IEC 2382-34, *Information technology — Vocabulary — Part 34: Artificial intelligence — Neural networks*

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

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

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
access
right, opportunity, means of finding, using or retrieving recorded information

3.2
accountability
principle that individuals, organizations and the community are responsible for their actions and may be required to explain them to others

3.3
admissibility
legal issue by which recorded information is determined to be acceptable as evidence in legal proceedings

3.4
agent
Person acting for another Person in a clearly specified capacity in the context of a business transaction

NOTE Excluded here are agents as "automatons" (or robots, bobots, etc.). In ISO/IEC 14662-01, "automatons" are recognized and provided for but as part of the Functional Services View (FSV) where they are defined as an "information processing domain (IPD)."

[CAN/CSA-ISO/IEC 15944-1-04]

3.5
audit
examination of systems, data centre procedures, programming and system usages to determine the authenticity, security and efficiency of recorded information and systems in accordance with a predefined policy or set of criteria

3.6
audit trail
chronological record of system activities that is sufficient to enable the reconstruction, reviewing and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results

3.7
authentication
provision of assurances of the claimed identity of an entity

NOTE Authentication is the process for testing the identities that applies to all entities involved in information and IT processes, including systems, system components and users, and any information captured, stored and retrieved from systems.

3.8
authentic
(in evidentiary proceedings) genuineness of a record, which in turn means the validity or authority of its authorship

NOTE It requires proof that a record is what it purports to be (that a record actually comes from the person, organization or other legal entity asserting to be its author or authorizing authority)

3.9
authenticity
property that ensures that the identity of a subject or resource is the one claimed

NOTE Authenticity applies to entities such as users, processes, systems, and information

[CAN/CSA-ISO/IEC TR 13335-1-01]

3.10
authorized
appointment, procedure or process formally approved by the judicial body of an organization that has the right or ability to make such commitments

3.11
backup copy
copy that is any of the following:

a) additional resource or duplicate copy of data on different storage media stored off-line for emergency purposes;

b) disk, tape or other machine-readable copy of a data or program file;

c) data or program file recorded and stored off-line for emergency or archival purposes;

d) record that preserves the evidence and information it contains if the original is not available

3.12
business transaction
predefined set of activities and/or processes of Persons which is initiated by a Person to accomplish an explicitly shared business goal and terminated upon recognition of one of the agreed conclusions by all the involved Persons although some of the recognition may be implicit

3.13
classification
(of records) systematic identification and arrangement of business activities and records according to logically structured conventions, methods, and procedural rules, represented in a classification scheme

3.14
commitment
making or accepting of a right, obligation, liability or responsibility by a Person that is capable of enforcement in the jurisdiction in which the commitment is made

[CAN/CSA-ISO/IEC 15944-1-04]

3.15
consumer
buyer who is an individual to whom consumer protection requirements are applied as a set of external constraints on a business transaction

NOTE 1 Consumer protection is a set of explicitly defined rights and obligations applicable as external constraints on a business transaction.

NOTE 2 The assumption is that consumer protection applies only where a buyer in a business transaction is an individual. If this is not the case in a particular jurisdiction, such external constraints should be specified as part of scenario components as applicable.

NOTE 3 It is recognized that external constraints on a buyer of the nature of consumer protection may be peculiar to a specified jurisdiction.

[CAN/CSA-ISO/IEC 15944-1-04]

3.16
conversion see also 3.21 3.38
process of changing records from one medium to another or from one format to another

3.17
corporate records officer
CRO
organization Person authorized to act on behalf of the organization and entrusted for overall governance of the electronic record management program and related programs

3.18
data
(in evidentiary proceedings) representations of information or of concepts, in any form

[CEA, section 31.8]

3.19
data element
unit of data for which the definition, identification, representation, and permissible values are specified by means of a set of attributes

[CAN/CSA-ISO/IEC 11179-3-04]

3.20
data file
set of related electronic records stored under defined criteria for subsequent storage and retrieval of the recorded information

3.21
data migration
moving sets of recorded information from one IT System or device to another, as required by changes in a system configuration or as requested by the user, while assuring that the data will be addressable and that data integrity will be maintained in the new environment

3.22
destruction
process of eliminating or deleting records, beyond any possible reconstruction

See also 3.31, *expungement.*

3.23
disposition
(of records) range of processes associated with implementing records retention, destruction or transfer decisions, which are documented in disposition authorities or other instruments

3.24
document
recorded information or object that can be treated as a unit

See also 3.49, *recorded information.*

3.25
Electronic Data Interchange
EDI
automated exchange of any predefined and structured data for business purposes among information systems of two or more Persons

3.26
electronic document
electronic record
set of recorded information (SRI) that is recorded or stored on any medium in or by a computer system or other similar device and that can be read, perceived or heard by a person or a computer system or other similar device

NOTE This definition is harmonized with the CEA's.

3.27
records management system
RMS
information system primarily designed to assist an organization in managing its recorded information concerning its record-keeping practices from inception to disposition of records

NOTE The system includes a means to demonstrate that procedures are in place to maintain the integrity and the authenticity of electronic records.

3.28
electronic signature
signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with an electronic document

[PIPEDA, Part 2, section 31(1)]

3.29
encryption
operation by which plain text is modified with an unintelligible, non-exploitable text making it non-retrievable except by authorized users that have the key to bring it back to its original form

3.30
evidence
information contributing to the proof of a fact

3.30.1
admissible evidence
evidence that is accepted in legal proceedings by the presiding judge or officer as not being excluded by any rule of evidence

3.30.2
relevant evidence
evidence that has any tendency in reason to prove a fact in issue in a proceeding

3.31
expungement
process of eliminating completely, wiping out, destroying or obliterating an electronic record

See also 3.22, *destruction*.

3.32
independent audit
audit performed by a person or persons acting independently, with no personal interest in the outcome of the results, who may be an employee(s) of the organization if that person(s) did not design, build, operate or manage the system

3.33
indexing
process of establishing access points to facilitate retrieval of records or information or both

3.34
integrity
(of records) reliability and trustworthiness of records as copies, duplicates or comparable representations of electronic records; and reliability and trustworthiness of the RMS in which it was recorded or stored to produce reliable and trustworthy copies and duplicates of electronically stored records

NOTE 1 The term integrity is used in the electronic records provisions of the evidence acts in the phrases "the integrity of the electronic records system" and "the integrity of the electronic record." However, the term integrity is not defined. In the absence of a statutory or judicially created definition, the principles of this standard shall serve as an operational definition of the word integrity used in the evidence acts.

NOTE 2 Certain evidence acts provide that the integrity of the electronic record may be proved by evidence of reliable encryption.

3.35
life cycle
(of records) stages in the life cycle of a record include but are not limited to its planning, creation and organization; the receipt and capture of data; the retrieval, processing, dissemination and distribution of data; its storage, maintenance and protection; its archival preservation or destruction or expungement

3.36
medium
physical material which serves as a functional unit, in or on which information or data is normally recorded, in which information or data can be retained and carried, from which information or data can be retrieved, and which is non-volatile in nature

NOTE 1 This definition is independent of the material nature on which the information is recorded and/or technology utilized to record the information, (e.g., paper, photographic, (chemical), magnetic, optical, integrated circuits (ICs); as well as other categories no longer in common use such as vellum, parchment (and other animal skins), plastics, (e.g., bakelite or vinyl), textiles, (e.g., linen, canvas, metals, etc.).

NOTE 2 The inclusion of the "non-volatile in nature" attribute is to cover latency and records retention requirements.

NOTE 3 This definition of "medium" is independent of

a) form or format of recorded information,

b) physical dimension and/or size, and,

c) any container or housing that is physically separate from material being housed and without which the medium can remain a functional unit.

NOTE 4 This definition of "medium" also captures and integrates the following key properties:

a) the property of a medium as a material in or on which information or data can be recorded and retrieved;

b) the property of storage;

c) the property of physical carrier;

d) the property of physical manifestation, i.e., material;

e) the property of a functional unit; and,

f) the property of (some degree of) stability of the material in or on which the information or data is recorded.

3.37
metadata
data about data elements, including data descriptions, and data about data ownership, access paths, access rights and data volatility describing records, records system, documents or data, including but not limited to the evidentially significant facts of:

a) their contents, definition, function, logical and physical structure, retention and disposition;

b) their sources of origins;

c) their relationships with other entities; and

d) any additional evidentially significant facts regarding their creation, acquisition, modification, maintenance, and use, including those individuals or organizations that have been active in or otherwise responsible for those activities, and their mandate or purpose for having been so engaged

3.38
migration
act of moving records from one system to another while maintaining the records' authenticity, integrity, reliability and usability

See also 3.21, data migration

3.39
organization Person
organization part that has the properties of a Person and thus is able to make commitments on behalf of that organization

NOTE 1 An organization can have one or more organization Persons.

NOTE 2 An organization Person is deemed to represent and act on behalf of the organization and to do so in a specified capacity.

NOTE 3 An organization Person can be "natural person" such as an employee or officer of the organization.

NOTE 4 An organization Person can be a legal person, i.e., another organization.

[CAN/CSA-ISO/IEC 15944-1-04]

3.40
Person
entity, i.e., a natural or legal person, recognized by law as having legal rights and duties, able to make commitment(s), assume and fulfil resulting obligation(s), and able of being held accountable for its action(s)

NOTE 1 Synonyms for "legal person" include "artificial person," "body corporate," etc., depending on the terminology used in competent jurisdictions.

NOTE 2 Person is capitalized to indicate that it is being utilized as formally defined in the standards and to differentiate it from its day-to-day use.

NOTE 3 Minimum and common external constraints applicable to a business transaction often require one to differentiate among three common subtypes of Person, namely "individual," "organization," and "public administration."

[CAN/CSA-ISO/IEC 15944-1-04]

3.41
Person identity
the combination of persona information and identifier used by a Person in a business transaction

[CAN/CSA-ISO/IEC 15944-1-04]

3.42
Person signature
a signature, i.e., a name representation, distinguishing mark or usual mark, which is created by and pertains to a Person

[CAN/CSA-ISO/IEC 15944-1-04]

3.43
preservation
processes and operations involved in ensuring the technical and intellectual survival of authentic records through time

3.44
probative value
weight or credibility given to evidence

See also 3.58, *weight*

3.45
procedures manual
(for records management) source of instruction and reference for the personnel responsible for creating, receiving, preparing, processing, storing and disposing of records

3.46
process
a series of actions or events taking place in a defined manner leading to the accomplishments of an expected result

[CAN/CSA-ISO/IEC 15944-1-04]

3.47
Quality Assurance Program
QAP
set of procedures based on the specifications of the RMS, which allow for monitoring and assessing its quality

3.48
record
information created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business

See also 3.49, *recorded information*.

3.49
recorded information
information that is recorded on or in a medium irrespective of form, recording medium or technology utilized, and in a manner allowing for storage and retrieval

NOTE 1 This is a generic definition and is independent of any ontology, (e.g., those of "facts" versus "data" versus "information" versus "intelligence" versus "knowledge," etc.).

NOTE 2 Through the use of the term "information," all attributes of this term are inherited in this definition.

NOTE 3 This definition covers:

a) any form of recorded information, means of recording, and any medium on which information can be recorded; and

b) all types of recorded information including all data types, instructions or software, databases, etc.

[CAN/CSA-ISO/IEC 15944-1-04]

3.50
records management
field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of, and information about, business activities and transactions in the form of records

3.51
retention period
specified period of time that records are kept to meet operational, legal, regulatory, fiscal or other requirements

3.52
secure environment
environment that precludes unauthorized access, mischief or physical disaster

3.53
set of recorded information
SRI
recorded information of an organization or public administration, which is under the control of the same and which is treated as a unit in its information life cycle

NOTE 1 A SRI can be a physical or digital document, a record, a file, etc. that can be read, perceived or heard by a person or computer system or similar device.

NOTE 2 A SRI is a unit of recorded information that is unambiguously defined in the context of the business goals of the organization, i.e., a semantic component.

NOTE 3 A SRI can be self-standing (atomic), or a SRI can consist of a bundling of two or more SRIs into another "new" SRI. Both types can exist simultaneously within the information management systems of an organization.

3.54
source record
record containing information or data entered into an RMS

3.55
storage
retention of data in a storage device

[ISO/IEC 2382-12:1988]

3.56
transitory record
record that is required only for a limited time to ensure the completion of a routine action or the preparation of a subsequent record

3.57
trouble log
comprehensive documentation identifying the various breakdowns and errors, including those associated with hardware, software, operating systems and application software, that have occurred within a system, and their associated repairs

3.58
weight
(in evidence) credibility or probative value of evidence

NOTE 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.

[CAN/CGSB-72.11]

4 Abbreviated terms

The following abbreviations are used in this standard:

CRO corporate records officer

EDI Electronic Data Interchange

IT Information Technology

QAP Quality Assurance Program

RMS records management system

SRI set of recorded information

5 Legal requirements for electronic records as documentary evidence

5.1 General

In the federal, provincial and territorial jurisdictions, the laws of evidence applying to legal proceedings permit computer-produced records, including electronic images, to stand in place of original paper source records or copies of paper source records. To prove the reliability of electronic records (computer-produced), the supporting or "foundation" evidence shall provide a detailed description of the RMS procedures used to record and store them. Two important assurances are thus provided by the current law that were not provided by the law before it was amended to accommodate electronic records[1]:

a) Reliable computer-produced records, including electronic images (see CAN/CGSB-72.11), are considered equal to original paper source records in legal proceedings.

b) Original paper source records can be disposed of once their electronic form is stored in a secure records management environment. Copies produced from these electronic records will have a legal authority equal to the original paper source records. **However, apart from the laws of evidence, other laws, regulations, by-laws, policies, preservation or business requirements might continue to require the retention of the original paper source records. An organization should consult a lawyer and its CRO before any source records are disposed of.**

NOTE The reader should be aware that regulation may require this section to apply to all legal proceedings, including those before administrative tribunals, and to request by taxing and other governments authorities requiring electronic records that satisfy the same requirements as those used by the courts.

---

[1] The model legislation that is the source of legislative language for enacting electronic records provisions into all evidence acts is the UEEA (see Annex B).

5.2 Outline of requirements for admissibility of electronic records as documentary evidence

5.2.1 Those who wish to present an electronic record as evidence in legal proceedings **shall** be able to prove

a) authenticity of the record;

b) integrity of the RMS that a record was recorded or stored in; and

c) that it is "a record made in the usual and ordinary course of business" or that it is otherwise exempt from the legal rule barring hearsay evidence.

The first requirement concerns the rule of authorship; the second, "the best evidence rule" — the rule of evidence concerning copies, duplicates and other substitutes for an original record; the third, "the hearsay rule" — the rule concerning the truth of the contents of a record. All evidentiary issues about the admissibility of a record or its weight involve one or more of these three rules. Admissibility concerns the acceptance of evidence, either testimonial or real (physical), in legal proceedings.

5.2.2 Authenticity involves whether a record is actually what it purports to be, i.e., its actual authority to "speak for" or represent its purported author regarding the data it contains. Authenticity requires proof that a document actually comes only from the person, organization or other legal entity asserting to be its author or authorizing authority.

5.2.3 The electronic record provisions of most of the evidence acts state that where the best evidence rule applies to an electronic record, it is satisfied by proof of the integrity of its electronic records system. Therefore, proof of the integrity of an electronic record is established by proof of the integrity of the RMS that recorded or stored it. This can be thought of as the "system integrity test" of admissibility for electronic records. In the absence of evidence to the contrary, such system integrity can be proved by evidence that

a) the computer system was operating properly; or if it was not, the fact of its not operating properly did not affect the integrity of the electronic record, and there are no other reasonable grounds to doubt the integrity of the electronic records system;

b) the electronic record was recorded or stored by a party to the proceedings that is adverse in interest to the party seeking to introduce it as evidence; or

c) the electronic record was recorded or stored "in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record" as evidence;

d) a printout of an electronic record that has been "manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout is the record for the purposes of the best evidence rule," i.e., the best evidence rule for paper documents applies since the printout is not being used to show the contents of a computer. In Alberta and Ontario, the evidence acts allow a party to support the integrity of the electronic record by showing that a reliable encryption system was used to create it.

5.3 The procedures manual

Senior management should require by by-law or formal policy directive that its organization have a manual outlining its RMS procedures (see Annex C). This manual should set out policies and procedures that provide evidence to satisfy the requirements for the admissibility of electronic records in legal proceedings:

a) a record made in the usual and ordinary course of business;

b) the circumstances surrounding the creation of the record;

c) the integrity of the electronic records system; and

d) the integrity of the electronic record.

The procedures manual can provide very persuasive evidence of an organization's usual and ordinary course of business about record keeping. Therefore, it is important that the procedures manual be authorized by senior management and not merely by the CRO.

5.4 How the procedures manual facilitates using electronic records as documentary evidence

5.4.1 In the event of legal proceedings (or a request by a taxing or other government authority), the procedures manual can be the most important support to satisfy the legal requirements (admissibility and weight) for electronic records in the evidence acts. The procedures manual can be used by a witness as evidence to prove that

a) an authorized RMS program is followed;

b) the RMS program provides proof of the system's integrity, i.e., the system reliably records, stores and processes electronic records; and, therefore,

c) the electronic records are authentic and have integrity, so trustworthy and reliable documentary evidence can be produced from them at any time and for any purpose.

5.4.2 An organization's records system, and its records, may be at risk of not being accorded evidentiary value if the records system has not been authorized and given formal support. The procedures manual should be created and implemented by a corporate by-law or by an order of comparable authority within the organization. The by-law or order should

a) order the creation and maintenance of the organization's RMS and record-keeping system (or give authoritative recognition to a pre-existing system);

b) order the creation and maintenance of the procedures manual;

c) create the position of CRO (or give authoritative recognition from senior management to a pre-existing position);

d) order that the records system comply with the procedures manual, the law, and national and industry standards so that the system can always produce its records as evidence;

e) require that the CRO obtain authorization to make major changes to the records system;

f) ensure that the CRO integrates the records system into the organization's usual and ordinary course of business, and maintains that integration; and

g) grant the CRO the exclusive power and responsibility to maintain and amend the procedures manual so that it continuously reflects the exact state of the records system and, more importantly, so that the procedures manual is the most important piece of evidence proving the system's compliance with the law and with national and industry standards.

5.4.3 Senior management, the organization's own internal law-making authority, proclaims throughout the organization the integrity of the organization's records system (and, therefore, the integrity of its electronic records) by establishing and declaring:

a) the system's role in the usual and ordinary course of business;

b) the circumstances under which its records are made; and

c) its prime directive for all RMS purposes, i.e., an organization shall always be prepared to produce its records as evidence. This dominant principle applies to all of the organization's business records including electronic, optical, original paper source records, microfilm and other records of equivalent form and content.

The procedures manual should be kept up-to-date and accurately reflect the exact nature, procedures and practices of the organization's RMS, i.e., the usual and ordinary course of business of that organization.

5.5 Proof of system integrity, record integrity and a record made in the usual and ordinary course of business

The following can be used to prove an organization's usual and ordinary course of business, the integrity of its electronic records system and, therefore, the integrity of any record recorded or stored in that system:

a) Sources of data: The organization creating the data;

b) Contemporaneous recording: The electronic records were captured and recorded contemporaneously with, or within a reasonable time after, the events to which they relate (but contemporaneous recording within a particular data base is not required);

c) Routine business data: The data within a record is of a type regularly supplied to the originating organization or created by it during its regular activities;

d) Data entry: The data-base capture and entry procedures are part of the usual and ordinary course of business of the organization and are carried out in accordance with the procedures manual;

e) Industry and national standards: The organization conforms to all appropriate standards for an RMS: inputting, importing and storing data, and preserving the reliability of data and of the RMS that stores and transmits the data;

f) Business reliance: The organization, when making business decisions, relies upon the electronic records in its data bases;

g) Software reliability: The software reliably processes the data;

h) Recording of system changes: A record of system changes is kept; and,

i) Security: Security features are used to guarantee the integrity of the RMS; at least, the following security features should be able to be proved:

   1) protection against unauthorized access to data and permanent records;

   2) processing verification of data and information in records;

   3) safeguarding of communications lines;

   4) maintenance of backup copies of records to replace falsified, lost and destroyed permanent or temporary records;

   5) retention and disposition of electronic records in compliance with legislated and internal retention periods and disposition requirements, and documenting such compliance and disposition schedules; and

   6) establishment of a business continuity plan for electronic records and associated data, including off-site copies of essential files, operating and application software.

The above factors should be able to be proved by a single supervising officer of the organization who is accountable for the records system. An additional witness may be required for software unique to the system unless the supervisor can prove its history of reliability. If not, the programmer who wrote the software should be available to certify its reliability until the software does have a history of reliability. The programmer or developer shall obtain a security clearance from the organization. Therefore, in choosing suppliers and programmers, consideration should be given to their ability and experience to prove the reliability of their products. And in legal proceedings, the use of data from an electronic record should not violate any legal principles prohibiting the disclosure of privileged or confidential data.

5.6 Use of the standard

5.6.1 In legal proceedings, this standard may be used to

a) develop arguments about what should be contained in the definitions of the four key phrases of the rules of admissibility for electronic records. These phrases are "system integrity" and "record integrity," as used in the electronic record provisions of the evidence acts, and "the usual and ordinary course of business" and "the circumstances of the making of the record," as used in the business and banking record provisions;

b) determine what evidence should be assembled for legal proceedings; and,

c) serve as a framework for developing examinations-in-chief of supporting witnesses (proponents of the electronic evidence), cross-examinations of opposing witnesses, and affidavits for all witnesses.

5.6.2 As an exhibit in legal proceedings, the standard would help determine

a) evidence and arguments to accept as relevant and admissible, and their weight;

b) definitions to use, i.e., the principles and practices to accept as essential elements of the four key phrases determining the admissibility and the weight of electronic records; and

c) appropriate scope of questions used in the examinations of witnesses — examinations-in-chief and cross-examinations.

6 Establishing a Records management system (RMS) program

6.1 General

Electronic record-keeping policies, procedures, programs, systems and processes all play important roles in the RMS infrastructure. This infrastructure, whose establishment is based on principles of good practice for records management, shall demonstrate that an appropriate RMS program has been adopted by the organization and that it is a part of the organization's usual and ordinary course of business.

This infrastructure provides basic requirements that enable the creation of appropriate procedures and controls to complement current standard operating-procedures or to guide in the development of the RMS program. These requirements include

a) establishment of the RMS program; - 6.2

b) policy definitions and responsibilities; 6.3

c) proper procedures and related documentation; 6.4

d) close alignment with information programs and technology, and effective implementation of system technologies;

e) information security; 6.12

f) implementation of a QAP; and - Section 7

g) audit trail. - Section 8

6.2 Establishing the program (organizational accountability)

6.2.1 Authorization

The establishment of an RMS program shall be authorized by corporate policy, executive order, by-laws or another instrument of comparable authority. The authorization shall confirm that the RMS program

forms part of the organization's **usual and ordinary course of business**. In addition to designating an organization Person as the appropriate signing officer or authority, the authorization **shall** include the following:

a) purpose of the record-keeping program;

b) implementation of a RMS program;

c) creation and establishment of a process for managing the retention and disposal of records;

d) establishment of a QAP;

e) establishment of an audit program; and

f) method of recording and certifying that the preceding activities are, in fact, carried out.

6.2.2 Responsibility

6.2.2.1 The CRO **shall** be clearly defined in the organization's **by-laws or instruments** of comparable authority to implement the RMS program in the **usual and ordinary course of business**. The organization shall identify any other delegated responsibilities and compliance to this program.

6.2.2.2 Delegation of responsibility to an agent

A Person **may carry** out an RMS program alone or may delegate all or part of an RMS program to an agent. In any delegation, the roles and responsibilities of the agent **shall** be clearly specified and documented to ensure that the integrity and authenticity of the electronic records are not compromised.

6.2.2.3 External service provider

Where an individual or organization uses a contracted external service provider to carry out all or part of an RMS program, the external service provider **shall** comply with the policy and procedures of the RMS program and shall be included in any contractual document.

6.2.2.4 Use of external service provider services

In this standard, the procedures and recommendations shall cover any type of service, including facilities management, document conversion and electronic record storage. The provision of application services is intended to ensure that the external service provider complies with the appropriate corporate policy and procedures. The individual or organization, when required, should also hold a copy of, or have access to, the external service provider's proof of compliance.

When storing information, agents **should** follow the relevant procedures and **should** be able and prepared to demonstrate in legal proceedings the effectiveness and security of their services.

6.2.2.5 Changes to the records management system (RMS) program

The organization **shall** authorize any changes and revisions to the RMS program.

6.3 Records management system (RMS) program policy

6.3.1 Requirements

An organization shall have a policy, an instrument or by-laws stating that electronic records are part of its usual and ordinary course of business.

6.3.2 Contents of the policy

The RMS program policy shall be part of and consistent with an organization's security policy for its RMS. The RMS program policy shall contain statements on

a) information and records covered under the policy or by-laws, including operating systems, applications software and communications infrastructure;

b) enabling technologies, their management and use in the life cycle of the recorded information;

c) data file formats and version control;

d) relevant RMS and technology standards, and their use within the organization;

e) entity and attribute definitions;

f) quality assurance;

g) metadata capture and preservation (including all evidentially significant information about records held by the organization, and the physical and logical structure of its information systems and communications infrastructure);

h) security classification and the method of and criteria for implementation;

i) security processes and procedures, in accordance with a formal RMS security policy, including:

   1) user authentication and permissions control;

   2) firewall protection;

   3) system backups;

   4) disaster recovery;

j) retention and destruction policies;

k) roles and responsibilities for all personnel managing and monitoring compliance with this policy; and

l) scheduled system and procedure audits for compliance to this policy and legislation.

All documentation shall be kept up to date.

6.3.3 Compliance with the policy

Compliance with the policy requires the following:

a) authorize the person or position responsible for obtaining and maintaining such compliance;

b) identify the appropriate legislation, directives and regulations that the responsible individual or job function should comply with;

c) identify all or part of any relevant national or international standards that should be complied with, and

d) identify how the organization complies with all applicable directives, legislation and regulations.

Periodic audits shall be conducted in accordance with sections 7 and 8 to verify compliance.

6.4 Records management system (RMS) procedures manual

6.4.1 General

Each Person that implements an RMS program shall have a complete and coherent set of authorized procedures documenting each aspect of its program, and the contents are to be managed centrally (e.g., through a consolidated procedures manual where appropriate) to ensure consistency and completeness.

The manual shall describe the procedures for the creation, capture, receipt, registration, management and protection of records through their life cycle. The manual shall be available upon request, and the procedures shall be implemented before the manual is to be presented as evidence. This manual shall provide the most persuasive evidence of the usual and ordinary course of business.

6.4.2 Revisions to the records management system (RMS) procedures manual

Changes to the RMS program and procedures shall be authorized, documented and logged. The changes in the RMS procedures manual shall be distributed as authorized.

6.4.3 Documentation

The RMS program's procedures manual shall specify the operation and use of the RMS, including input, storage and output of records and data, and all procedures affecting the efficiency and security of the system. The manual should include references to other controlled documentation (e.g., other business procedures or systems documentation) as appropriate. The references shall be kept up to date. The manual shall have a formal review cycle to ensure ongoing alignment with other organizational requirements.

All persons using the RMS shall be aware of all procedures that relate to their responsibilities, and these procedures and other relevant documentation shall be available to authorized users of the system.

6.4.4 Preservation of life-cycle metadata

The preservation of life-cycle metadata, which forms an integral part of record keeping, shall be authorized by the organization. The purpose of life-cycle metadata is to assure future interpretation and trustworthiness of the electronic records, despite changes in technology over time. The preservation of

life-cycle metadata shall include a complete history of the activities occurring and the parties involved at each event within the life cycle of records (and the data contained therein). Preservation shall also include creation, revision, reformatting, copying, transformation, conversion, migration and disposition. The life-cycle metadata shall also include a complete description of the system's contents and design architecture including all logical and physical models as implemented, complete entity and attributed definition, and a precise account of the use of operating systems and program application.

6.4.5 Data capture

Data forming the contents of electronic records may be created by the organization through its RMS program or imported into it from an external source. Documented control procedures shall exist for both types of capture, and a QAP implemented that is timely to the capture event. Minimum quality levels covering accuracy and completeness of captured data shall be specified.

A complete set of metadata including all evidentially relevant information on the source of the data, the business rules associated with its capture (creation), its logical structure, and complete entity and attribute definitions shall be captured or created. This metadata shall be kept in a secure environment for the life cycle of the document.

6.4.6 Data migration and data conversion

To ensure the integrity of the data being moved, data migration or conversion procedures shall include data testing, validation and final sign-off by all stakeholders, e.g., an authorized person or position within the organization and any agent providing migration or conversion services. All previous audits, metadata and indexing associated with the source system shall be preserved so that the integrity of the data can always be established.

When transformations occur to meet business and data management needs (e.g., sampling or aggregations of data, or data cleansing associated with QAP), policies and procedures shall document the associated rules and processes.

6.5 Indexing

6.5.1 General

Indexing is a vital part of storing and retrieving information on an RMS program. Indexing, which can be automated or manual, shall include the following functional requirements:

a) the specification of the indexing methodology and schema used;

b) type and structure of indexing used, including the primary index element as well as all additional levels of indexing;

c) methods for performing quality control of indexing;

d) procedures in place to amend inaccurate index data;

e) where an index entry references deleted or expunged information, the index shall reflect the deleted or expunged status; and

f) procedures for performing quality assurance of the indexing.

6.5.2 Index retention, rebuilding and recovery

Index data shall be kept for the retention period of the SRI to which it relates. The procedures for rebuilding an index, changing an index structure, and recovering a damaged or faulty index shall be authorized and documented, as well as all results of such events.

6.6 Authenticated output of paper copies for legal proceedings

6.6.1 Whenever paper copies need to be produced from an RMS, those copies need to be authenticated as true copies of the originals to enhance their admissibility and weight in legal proceedings. The procedures for producing and authenticating paper copies shall be documented.

Where a paper document is produced as part of the output, the procedures shall include the use of an authorized Person signature or other authorized procedure to authenticate this document.

When layout of the paper output and the original document differ, the nature of the differences and the manner in which they occur shall be authorized and documented.

6.6.2 Authentication of copies of data files

Whenever several parties simultaneously hold copies of a data file or provide input into a data file, authorized procedures for authenticating copies of data files shall be documented.

6.7 Data transmission

When data are being transmitted between systems, a procedure shall be set up to detect interference that could corrupt data integrity.

The date and time of any data transmission received or sent shall be logged as part of the audit trail.

Where it is important to be able to demonstrate that the data have been delivered, the acknowledgement of the transmission identifier should be retained.

The level of security risk being taken during an external data transfer should be assessed to ensure compliance with the requirements of the organization's security policy.

6.8 Record retention requirements

The time period that records shall be retained shall be determined by authorized persons within an organization, i.e., an organization Person (normally those persons responsible for the organizational functions that the records support). The assignment of the responsibility for records retention requirements to an organization Person shall be formally documented.

The retention times vary with record functions and are generally based on business requirements for access to the information and on any legal and audit requirements. Record retention requirements are (1) those of a general nature applicable to any Person including their financial records; and (2) those arising from the nature of the goods, service or right being provided by an organization. For example, when the client of an organization is an individual, i.e., a consumer, a specific record retention requirement arising from consumer protection requirements may apply to the organization in its role as a vendor. Similarly, where the nature of the goods or service being provided necessitates meeting environmental requirements, additional or different records retention requirements may apply.

It is the responsibility of each organization to ensure that it has identified all the record retention requirements applying to its records and that these requirements are supported in its RMS.

The organization's record-keeping policy shall also define "transitory records" — records to which no record retention requirement applies and which have no value in documenting or supporting the organization's business. These records should be destroyed after initial use. The organization's RMS procedures should promote the systematic disposal of transitory records to ensure that only records of value to the organization are managed and kept.

6.9 Record disposition

6.9.1 General

When establishing an RMS, organizations should seek legal advice to ensure that they fully comply with legislation (and pursuant regulations) covering the disposition of records or regulating their amendment, i.e., changing the contents of an existing record.

6.9.2 Disposal of electronic records

Disposal of a record shall occur after the appropriate retention period has expired. An organization shall be capable of documenting a disposal when proof of destruction is warranted or required, based on business, legal and audit requirements.

Disposal of records and metadata means either destruction or transfer to another entity, i.e., remove from under the control of the organization. In either case, documented proof such as an audit log, a certificate or evidence of disposal is required. Such certification should identify the records disposed (using the associated metadata), the nature of records (e.g., subject classification code), the date the records were created or received, the person who authorized the disposal, and the time and date of disposal. This record of disposal actions should be kept by the organization as proof of disposal. Metadata will sometimes be retained after their referring records have been disposed of; the metadata should then record the event of disposal.

6.9.3 Deletion of electronic records

System transaction logs, audit trails and other appropriate records of deletion and amendment transactions should be retained.

There may be a requirement to expunge a specific record from an RMS because of legal or administrative requirements, particularly in accordance with privacy regulations or other legislation. The RMS should have facilities to delete, expunge, amend or correct records using an editable process. System procedures should also ensure that both the record and the index locator are expunged to prevent recapture (re-creation) of the record and index locator.

Where deletion of any record from an RMS occurs, appropriate authorization shall first be obtained, usually through an authorized instrument such as a records retention schedule. The authority for approving these instruments and for deciding when not to proceed with scheduled disposals should be included in the by-laws or administrative policies of the organization, and these responsibilities assigned to a specified organization Person. System procedures should state that only the organization Person so authorized may register or implement these decisions.

6.10 Backup and system recovery

Effective procedures for the backup of electronic records and data files and all associated information (e.g., index files and audit trails) **should** be included in the RMS procedures manual. Only authorized Persons **shall** be allowed to enable or disable the backup and recovery functions.

The RMS recovery procedures **shall** be documented in order to demonstrate that such procedures are controlled and tested for reliability and that data file integrity has not been compromised after restoration. The storage media **shall** be tested to prove that ~~the~~ no recorded information or metadata have been lost. Backup media shall be tested at predetermined intervals for accuracy and integrity of data.

A backup log **shall** be kept in the system's audit trail of all backup and recovery activities, including any problems incurred during the procedure.[2]

The procedures manual **shall** include the procedures for moving a backup copy to and from an off-site facility.

If the structure of the data files held on a backup copy differs from that of the originals, the structure of the backup copy **shall** be documented.

Where backup data are used to recover from a system failure, procedures **shall** be documented to ensure that data file integrity has not been compromised.

Backup procedures and details about transfers **shall** be retained for as long as the referring data or records are required.

6.11 System management guide

All significant details of the logical and physical architecture of an RMS **shall** be fully documented including the accountabilities and the relationships between system design and conduct of the organization's business. The RMS management guide **shall** be structured so that the integrity of the system can be demonstrated for any point in time. The documentation required for an RMS **shall** include the following:

a) description of the hardware, software and network elements that comprise the system and how they interact;

b) defined procedures, including event scheduling and accountabilities, for monitoring and maintaining systems and data integrity and for taking preventive and corrective action where required;

---

[2] It is prudent to have several simultaneous backup copies of data and application programs and to maintain one of these at another location.

c) trouble logs, schedules and procedures for assessing the system's ongoing operational integrity and for taking corrective action where required;

d) documentation of changes to the system including all responsible persons and a full account of the processes and activities undertaken to affect the change; and

e) procedures to control the use of system maintenance hardware and software that can bypass system access controls shall be documented, and such hardware and software shall be used only as authorized.

6.12 Security and protection

6.12.1 Security procedures

Details of all levels of access available on the RMS and procedures for their use should be documented.

Procedures should be implemented in accordance with the organization's RMS security policy. These procedures should include notification of, and protection against, unauthorized access as well as guidelines on access and changes in personnel with access. Personal security screening of persons working for the organization shall be in accordance with the information's level of sensitivity.

The accommodation and operating environment for the RMS and for the storage, transportation and maintenance of data storage media should be in accordance with suppliers' recommendations and relevant national or international standards.

6.12.2 Encryption keys and digital certificates

Encryption should be used to improve the security and integrity of stored records.

Where electronic signatures are used, procedures shall be implemented for encryption key allocation and management and for certificate management. Encryption or electronic signature keys shall be valid, kept secure and made available only to authorized persons.

6.13 Workflow

Where workflow systems are implemented, operational details shall be documented in the RMS procedures manual. Such details should ensure that record integrity cannot be compromised during a workflow process.

Where changes to the workflow system are implemented, change-control procedures shall be implemented to ensure that stored records are not lost during the procedure.

6.14 Selfmodifying electronic records

6.14.1 Some electronic records may contain automatically executable codes, often referred to as macros, that can modify a file each time it is retrieved, viewed or printed (e.g., by inserting the current date and time). The existence of such codes within a file means that the file cannot be frozen. Each time the file is retrieved, it may appear to be different although the user has not changed the stored file.

To prove evidentiary value, organizations should implement procedures to prevent any form of automatic modification. These procedures should ensure that authentic copies of the original information can be produced.

6.14.2 Date and time stamps

Procedures for the regular checking of computer system clocks for accuracy concerning date and time keeping should be documented. Date-keeping and time-keeping procedures should include the ability to detect and correct errors. All actions taken concerning error correction or resetting of system clocks should be documented.

An organization should specify which personnel are authorized to access and modify system clocks, and ensure that appropriate access control measures are established.

6.15 Audio and video data

The procedures used for audio, video and multimedia data (digital format data) storage should be documented in the same manner as for all other data. Where the recording of the data is not under the control of the RMS program, the recording system should control data integrity.

6.16 Record version control

Procedures should be established for and incorporated within a record-keeping system to enable implementation of systematic version controls for all documents. These procedures should include definitions of when a record should be saved as a new version.

Accountability and procedures for changing previously stored records and data files should be documented (e.g., update procedures) as part of the system documentation.

A record version control-procedure should be established for all records.

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

7 Quality Assurance Program (QAP)

7.1 General

The QAP monitors and judges the RMS, including the quality control operations. A QAP shall be accurate, reliable and trustworthy, and meet its set objectives.

7.2 Procedures

Procedures shall describe the QAP used to check any part of the RMS. The QAP should rely on sampling, using best industry methods to calculate percentages by random sampling or through a detailed point-by-point inspection and verification. It should be performed at predetermined points within the operation or at periodic intervals. Procedures will vary from application to application and will be developed based on the relevance of the data, the urgency of providing the data, and the costs deemed appropriate to allow for the most effective verification of the data. Periodic confirmation reviews shall be conducted by independent audit to verify compliance.

8 Audit trail

8.1 General

When preparing electronic records for use as evidence, it is often necessary to detail the storage date of the information, the movement of the information from medium to medium, and the evidence of the controlled operation of the RMS. These details are known as audit trail information. In this standard, the audit trail shall consist of a historical record of all significant events associated with the RMS.

Procedures for audit trails and any changes to the accepted procedures shall be documented in an RMS procedures manual.

Audit trails shall contain sufficient and necessary information to provide evidence of the authenticity of stored records. The audit trail of an RMS shall consist of system-generated and operator-generated logs containing data about changes to the stored records. If the authenticity of stored records is questioned, the integrity of the audit trail may be fundamental in establishing the authenticity and therefore the evidentiary weight of the stored records.

8.2 Management of audit trail records

The audit trail shall be subject to internal records management procedures similar to those for other essential records of the organization. This requirement applies to audit trail data kept on electronic media, paper or microfilm. Audit trail data kept within the RMS should not be modifiable in the secure environment. Secure backup copies of the audit trail should be kept.

Records shall be kept in the audit trail that document essential information captured by or imported into the system. Sufficient information shall be stored for each processing procedure.

8.3 Content of audit trail

8.3.1 The organization shall establish the content of the audit trail to be used by all relevant departments. Typical audit trails consist of system-generated and operator-generated logs. Audit trails shall be kept on the events occurring on the RMS, including historical activities or events that in the future may need to be reconstructed as additional evidence to support stored records.

The audit trail shall contain data about changes to the records stored on the system. Audit trails shall contain sufficient and necessary information to provide evidence of the authenticity of the stored records.

8.3.2 The following are minimum content requirements:

a) system function applied;

b) objects to which the function was applied (including their unique identifiers);

c) outcome;

d) organization Person responsible for initiating and carrying out the function; and

e) date and time of events such as

1) initial capture of an electronic record or data element into the system;

2) creation of new electronic record versions;

3) initial and any subsequent assignments of an electronic record or data element to an internal or external location within the RMS;

4) changes in the RMS software;

5) record processing-events (e.g., aggregation of data and the formulas applied);

6) creation, amendment and deletion of metadata;

7) creation of and changes in access authorization for records or data;

8) creation of and changes in retention and disposal requirements;

9) assignment of a record security classification or changes to that classification; and

10) destruction of records or data.

8.3.3 Information stored in the audit trail for an imaging system shall include

a) process date and time stamp;

b) batch reference (for batch input);

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

d) QAP check approval;

e) identifier for each indexed record or file;

f) operator or work-station identifier; and

g) final write to storage.

Additional data to be stored in the audit trail record log shall depend on the application and the system. If file recovery procedures have been implemented, sufficient audit trail data should be stored to demonstrate that the recovery did not affect record authenticity.

8.4 Creation

Audit trail data should be generated automatically by the RMS, and the RMS procedures manual shall describe the processes. If audit trail data are not generated automatically by the RMS, the procedures for generating such data shall be documented in the RMS procedures manual. These procedures shall apply to the organization and any contracted external service providers.

The procedures to be followed when an audit trail data file becomes full (and the identification of this situation) shall also be documented in the RMS procedures manual.

8.5 Date and time

Each audit trail shall include the date and time that an event occurred. The date and time of a recorded event shall be accurate so that an investigation can determine the sequence of events. System-generated audit trail records shall be created when an event is recorded. The associated date and time will normally be that of the creation of the audit trail record. However, if this creation is made contemporaneously with an event that is being recorded, the time will usually be that of the event itself. A manually generated audit trail record shall be created as soon as possible after the event that is being recorded.

If the time that an event occurred is important, a valid time stamp should be used.

Audit trail data about the capture process provides invaluable information to help authenticate stored information. Details such as capture time, operator, capture device and type of original may prove vital if authenticity is challenged.

8.6 Storage

The storage of audit trail records shall form part of an organization's RMS policies. Audit trail records shall be included as a specific document type in the RMS policy document.

Audit trail records shall be stored in a secure environment for as long as the information that they refer to is required by the organization or by law.

8.7 Access

Audit trail information may need to be accessed by authorized personnel. In some applications, access may only be needed on an ad hoc basis, so it is important that the access and interpretation procedures are documented.

The RMS procedures manual shall describe how the audit trails can be accessed and interpreted.

8.8 Security and protection

If the authenticity of the stored records is questioned, the integrity of the audit trail may be fundamental in establishing the authenticity and, therefore, the evidentiary weight of the stored records.

The level of security for the audit trail should be appropriate for preventing any change to its data. Audit trail data should be stored securely in accordance with the security policy for the relevant RMS.

Secure backup copies of the audit trail should be kept for data on any medium and should be appropriate to that medium (e.g. electronic, paper or microfilm, as required).

Audit trail information kept in the RMS shall not be modifiable.

The audit trail data should be stored to demonstrate that the recovery did not affect data authenticity.

Paper documents used for audit trail data should be stored securely. Where paper documents are used, storing copies of them on the RMS is recommended.

8.9 Data migration and conversion in audit trail

8.9.1 If information is moved between storage devices as part of a data file migration process, details of the move shall be stored in the audit trail. Procedures for data migration or conversion shall include methods for proving that any related data (e.g., metadata) are also migrated or converted.

8.9.2 If data are routinely and automatically moved between storage devices without user intervention, audit trail data may not be required. It may be necessary to demonstrate that the storage management system was working normally when the data were transferred.

✳ **8.9.3** Where records have been converted from one file format to another, details of the conversion shall be stored in the audit trail log.

8.10 Workflow

Each time a new business process is defined or an existing definition is changed, an audit trail record should be generated. Where workflow systems exist, audit trail points for generating data should be defined.

In a typical workflow system, an audit trail point exists at each step in the workflow. For compliance with the policy and procedures manual, audit trail logs may not need to be kept for every audit trail point. The user should decide which audit trail points are relevant regarding the potential evidentiary importance of the data within the workflow. Those audit trail points should be selected for the generation of audit trail data.

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

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

8.11 Verification

Audit trail records shall be kept of activities or events that may need to be reconstructed in the future as additional evidence to support stored electronic records.

Annex A
(informative)

Sources of requirements and approach to CAN/CGSB-72.34

A.1 Introduction to annex

This annex sets out the sources of requirements that have been integrated into this standard.

CAN/CGSB-72.34 is based on the law of evidence for the admission of documents commonly referred to as documentary evidence. The law on this question is a mix of common law (the result of cases decided in the courts) and statutes. The common law on documentary evidence is similar across Canada, in the common law jurisdictions. The statute law is found in the federal, provincial and territorial evidence acts, which vary slightly. The basic rules for Quebec are found in the Civil Code of Quebec, notably Book Seven on Evidence, and, in particular, articles 2837 to 2842, and 2870.

Today, the general law of documentary evidence is supplemented in much of Canada by specific legislation dealing with electronic documents or records. (The statutes do not distinguish between electronic documents and records — the terms are used indifferently.) The principal, though not the only, source for this specific legislation is the **Uniform Electronic Evidence Act** (UEEA), adopted by the Uniform Law Conference of Canada in 1998, and now in force federally and in six provinces (Alberta, Saskatchewan, Manitoba, Ontario, Prince Edward Island, and Nova Scotia) and the Yukon Territory.

The relevant federal statute is the *Canada Evidence Act* (CEA). It was amended in 2000 by Part 3 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which added sections 31.1 through 31.8 to the CEA. Those sections are heavily influenced by the UEEA. The amendment was introduced and enacted as one initiative in support of the Canadian Electronic Commerce Strategy, which in turn aims to encourage widespread adoption of e-business.

The UEEA (see Annex B) in all its enactments provides that the integrity of an electronic record can be demonstrated by proving the integrity of the record-keeping system of which it is a part. In disputed cases, the integrity of the record-keeping system can be supported by reference to standards applicable to the system in question. Even in jurisdictions without the UEEA, courts are generally open to reference to applicable standards.

This standard is such a standard.

A.2 Sources of requirements

The sources of requirements for this standard, which are integrated or were taken into account in its development, include:

a) Canadian legal requirements, especially those of an evidentiary nature, including:

- legislation and pursuant regulations (federal, provincial, territorial);
- jurisprudence (results of court actions, legal proceedings, precedents).

b) key international standards on records management and e-business including:

- CAN/CSA-ISO/IEC 14662-01: *Information Technology — Open-EDI Reference Model*;

NOTE This is the framework standard for modelling business transactions from both the business operational view (BOV) — best business practices — and the functional services view (FSV) — the required information and communication technology support services. CAN/CSA-ISO/IEC 14662-01 serves as the basis for subsequent work of UN/CEFACT (United Nations Centre for Trade Facilitation and Electronic Business), ebXML, etc.

- ISO 15489-1, *Information and documentation — Records management — Part 1: General*;
- ISO/TR 15489-2, *Information and documentation — Records management — Part 2: Guidelines*

NOTE TR indicates technical report.

- CAN/CSA-ISO/IEC 15944-1-04, *Information technology — Business agreement semantic descriptive techniques — Part 1: Operational aspects of Open-edi for implementation*

CAN/CSA-ISO/IEC 15944-1-04 also incorporates the requirements of legal frameworks from an international perspective (including those of common law and civil law as well as other legal systems and international law). Increasingly known as the international e-business standard, it contains key terms and definitions that bridge the legal, commercial and IT worlds as well as public policy requirements (e.g., privacy and consumer protection) of any business transaction including those concerning Persons as individuals, and organizations and public administration making commitments (see 5.1.3 of CAN/CSA-ISO/IEC 15944-1-04):

i. individual <-> individual;

ii. individual <-> organization, a.k.a. as "B2C";

iii. individual <-> public administration;

iv. organization <-> organization, a.k.a. "B2B";

v. organization <-> public administration;

vi. public administration <-> public administration.

NOTE Although CAN/CSA-ISO/IEC 15944-1-04 is available in English only, it does contain an Annex A (normative) entitled "Consolidated list of terms and definitions with cultural adaptability: ISO English and ISO French language equivalency." Canada was a major contributor to this international standard, preparing the (draft) "ISO French Language Equivalents for the terms and definitions." This contribution in turn helps ensure that CAN/CSA-ISO/IEC 15944-1-04 meets and supports Canada's legal official language requirements.

c) ICT requirements and standards

Relevant elements of ICT requirements and standards that serve as a basis for this standard are found in Clause 2, "Normative references," of this standard. Other relevant ICT standards from a generic e-business perspective are found in Clause 2, "Normative references," of CAN/CSA-ISO/IEC 15944-1-04.

d) Business operation requirements and best practices (and related standards)

This standard also incorporates common operational requirements of organizations as well as best practices in records keeping, ensuring integrity of digital recorded information. The committee of experts that drafted this standard are drawn from well-known Canadian professional and industry associations in the areas of information, records and image management; legal and financial services; and accounting and auditing. The experts represent both user and supplier perspectives, ensuring a balanced approach in this CGSB standards committee.

A.3 Approach

The Canadian Electronic Commerce Strategy incorporates in its priorities for action the clarifying of marketplace rules by implementing the principle of "media-neutrality of statutes" (see p. 19). This principle is also applied in this standard. Key terms and definitions in this standard are IT neutral, i.e., they apply irrespective of the combination of information and communication technologies utilized.

This standard focuses on ensuring the integrity of recorded information generated and maintained in electronic form on IT Systems of an organization irrespective of whether the organization is private or public sector based or operates on a for-profit or not-for-profit basis. Implementation of this standard by an organization is a key element in ensuring that its recorded information, as supported through its IT System, is and remains reliable, authentic and trustworthy, particularly when:

a) the organization or public administration decides to transfer its applications from its existing IT System to a new IT System, i.e., the combination of hardware, software, data-base document management systems, etc., for its internal record-keeping practices;

b) the organization adds to or changes the means of communicating and interchanging its recorded information in support of its business transactions with other Persons, be these individuals, organizations or public administration. The most common example is that of an organization adding or switching to an Internet (WWW-based) interface;

c) a public administration adds to or changes the laws or regulations for which it is responsible by allowing its information reporting or interchange requirements to be met using EDI where such interchange of electronically recorded information is in support of activities that involve commitment exchange between the Persons, i.e., parties, concerned. This is commonly known as e-government.

Regarding these three examples, or combinations of these examples, this standard provides specific criteria that shall be maintained to ensure the admissibility of electronically recorded information as evidence in legal proceedings.

Further, this standard makes extensive use of CAN/CSA-ISO/IEC 15944-1-04, the international e-business standard that incorporates legal framework requirements from an international perspective.

There is a strong possibility that organizations implementing this standard will also benefit from a global perspective by removing legal obstacles from the introduction of electronically recorded information as evidence in legal proceedings.

A.4 Additional definitions

These definitions are provided for information only.

organization information
recorded information that is important to an organization

evidentiary metadata
metadata describing an SRI, including but not limited to the evidentiary significant requirements and resulting facts pertaining to:

a) their contents, definition, function, logical and physical structure, retention and disposition;

b) their sources of origins;

c) their relationships with other entities; and

d) any additional evidentially significant facts regarding their creation, acquisition, modification, maintenance and use, including those individuals or organizations that have been active in or otherwise responsible for those activities, and their mandate or purpose for having been so engaged.

Annex B
(informative)

Uniform Electronic Evidence Act

This annex reproduces the Uniform Electronic Evidence Act (UEEA) adopted by the Uniform Law Conference of Canada in 1998. The UEEA is a **model act** from which federal, provincial, and territorial acts are derived, but it **is not actual legislation federally, provincially or territorially.**

Definitions

1. In this Act,

a) "data" means representations, in any form, of information or concepts.

b) "electronic record" means data that is recorded or stored on any medium in or by a computer system or other similar device, that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data, other than a printout referred to in Subsection 4(2).

c) "electronic records system" includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording and storage of electronic records.

Application

2.(1) This Act does not modify any common law or statutory rule relating to the admissibility of records, except the rules relating to authentication and best evidence.

2.(2) A court may have regard to evidence adduced under this Act in applying any common law or statutory rule relating to the admissibility of records.

Authentication

3. The person seeking to introduce an electronic record [in any legal proceeding] has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

Application of the best evidence rule

4.(1) [In any legal proceeding,] Subject to Subsection (2), where the best evidence rule is applicable in respect of an electronic record, it is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored.

4.(2) [In any legal proceeding] An electronic record in the form of a print-out that has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, is the record for the purposes of the best evidence rule.

Presumption of integrity

5. In the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is presumed [in any legal proceeding]

a) by evidence that supports a finding that at all material times the computer system or other similar device was operating properly; or if it was not, the fact of its not operating properly did not affect the integrity of the electronic record, and there are no other reasonable grounds to doubt the integrity of the electronic records system;

b) if it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or

c) if it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

Standards

6. For the purpose of determining under any rule of law whether an electronic record is admissible, evidence may be presented [in any legal proceeding] in respect of any standard, procedure, usage or practice on how electronic records are to be recorded or stored, having regard to the type of business or endeavour that used, recorded or stored the electronic record and the nature and purpose of the electronic record.

Proof by affidavit

7. The matters referred to in Subsection 4(2) and Sections 5 and 6 may be established by an affidavit given to the best of the deponent's knowledge or belief.

Cross-examination

8.(1) A deponent of an affidavit referred to in Section 7 that has been introduced in evidence may be cross-examined as of right by a party to the proceedings who is adverse in interest to the party who has introduced the affidavit or has caused the affidavit to be introduced.

8.(2) Any party to the proceedings may, with leave of the court, cross-examine a person referred to in paragraph 5(c).

Repeal

9. [Repeal provisions which require retention of original after microfilming.]

September 1998

Annex C
(informative)

Content of records management system (RMS) procedures manual

In addition to a formal policy directive, the RMS procedures manual should include a description of the procedures and process for the topics listed below:

- Record types authorized for capture and maintenance by the RMS;
- Record types not authorized for capture or maintenance by the RMS;
- Record receipt processing;
- Record creation and capture;
- Document scanning;
- Data and record capture;
- Electronic document quality assurance;
- Indexing, registering and profiling;
- Authenticated output procedures;
- File transmission;
- Storage media in use;
- Electronic information retention;
- Electronic information disposition and destruction;
- Disaster–recovery programs;
- Backup and system recovery;
- System maintenance;
- Security, confidentiality, privacy and protection;
- Use of contract service provider services;
- Use of other trusted third parties;

- Workflow;
- Selfmodifying files;
- Audit trails;
- Voice, audio and video data;
- Version control;
- Change control and maintenance of documentation;
- Retention scheduling;
- Information disposition and destruction;
- Electronic information transformation between media;
- Procedure and technology change management procedures;
- Updating procedures for the procedures manual.

Annex D
(informative)

Bibliography

D.1 The publication referenced in 2.2 may be obtained from the Canadian General Standards Board, Sales Centre, Gatineau, Canada K1A 1G6, telephone (819) 956-0425 or 1-800-665-2472, fax (819) 956-5644, e-mail ncr.cgsb-ongc@pwgsc.gc.ca, Web site www.ongc-cgsb.gc.ca.

D.2 The publications referenced in 2.3 may be obtained from the Canadian Standards Association, Web site www.shopCSA.ca.

D.3 The publications referenced in 2.4 may be obtained from the Department of Justice Canada, Web site www.justice.gc.ca.

D.4 The publication referenced in 2.5 may be obtained from the Uniform Law Conference of Canada, Web site www.ulcc.ca.

D.5 The publications referenced in 2.6 may be obtained from IHS Canada, 1 Antares Drive, Suite 200, Ottawa, Ontario K2E 8C4, telephone (613) 237-4250 or 1-800-854-8220, fax (613) 237-4251, e-mail gic@ihscanada.ca, Web site www.ihscanada.ca.